Crypto Currencies: Should we trust?

Dimitris C. Zoumpakis [redacted]

Fundamentals of Information Systems

Dr. Katerina Papanikolaou

Department of Sciences, B.Sc. Computer Information Systems, European University Cyprus

28 November 2023

Table of Contents

Following recent collapse of giants such as FTX and the charges against the CEO Sam Friedman, days before the charges against Binance CEO and the burst of the NFT's (Non-Fungible Tokens) "bubble", rising from the rise of crypto millionaires that seem to multiply day by day and influencers such as Kevin O'Leary urging people to invest their money in cryptocurrencies such as Bitcoin using specific platforms, a very crucial question arises. That is the degree of trust between cryptocurrencies and an individual. The general lack of knowledge on such technologies in addition to several key elements highly influences trust, and trustworthy exchanges. It should be noted that the research of blockchain technologies thus the cryptocurrency ecosystem is led by industry rather than academia. Thus, lacking still, a comprehensive analysis of the direct or indirect issues affecting stakeholders. This paper explains cryptocurrency, blockchain and cryptography at a fundamental level as well as an overview of benefits and downgrades of cryptocurrencies which coherently affect trust following an overview of several models for trust analysis.

Beginning with understanding the basics of cryptocurrencies, just knowing that crypto represents a digital medium of exchange which enables distributed, decentralized, and secure economic transactions is not enough (Bucko, et. Al. 2015). A major distinction must be made clear between cryptocurrencies and cryptocurrency systems. A cryptocurrency system is a system built to issue tokens which are issued solely to be used as general or limited-purpose medium-of-exchange, using a collectively maintained digital ledger. Cryptocurrency refers to the token that has been issued by the cryptocurrency system (Pernice et. al, 2021). The term cryptocurrency would first appear in public eyes with a different name, as the project was introduced by the founder of Bitcoin (most valuable cryptocurrency as of today) Satoshi Nakamoto as a "peer-to-peer currency in a network and cryptography mailing list" (Nakamoto, 2008b). Even when the distinction between cryptocurrency and cryptocurrency system is made clear, another critical aspect of understanding the fundamentals of the crypto ecosystem is how new bitcoins are made or as called, crypto mining. This happens by a network participant, or so-called miner, who themselves have successfully transformed the format of a bundle of proposed transactions, which are previously issued bitcoins paired with a request to issue new ones as a reward and in this way the bundle can be added to the chain of previously added bundles which resonates with the basic principle of cryptocurrencies, which is that no one may accelerate or significantly abuse their production (Bucko, et. Al. 2015). Most purchases made with cryptocurrency tokens are in the form of countertrade, the token priced in fiat currency is then compared to a product or service priced in fiat currency and thus an exchange ratio emerges (Pernice et. al, 2021). Cryptocurrencies can also be bought for speculation, which means buying the token with fiat currency with the intention of reselling it for fiat currency which is proven to drive volatility in the fiat currency price of crypto tokens (Baur, Hong, and Lee, 2018). Another key ability of crypto is lowering costs of online transactions by removing the cost of third parties, as well as the transfer protocol which they deploy which, works fundamentally as that only the processor of a private key that can allow entry to an 'unspent transaction output' can initiate a transfer (Pernice et. al, 2021). However, cryptocurrency tokens are essentially blank digital tokens that would be almost featureless if it were not for the name and brand they are being promoted by. Moreover, crypto tokens are almost

entirely not accepted in exchange for goods and services in addition to not being used to price stuff, with one of the biggest downsides being that they struggle with storing value which simply means that we fiat currency you can easily predict the price of milk in a week or month or even year when with cryptocurrency you cannot. Cryptocurrency is not stable and in addition highly unregulated, with attempts in the past few years to create “stable coins” which are backed by assets that have fiat currency prices (Klemm, et al. 2019). As stated by Blandin (et al. 2019) such coins might be categorized as a modern form of digital currency since they could be regulated under laws for e-money, money-laundering etc.

To fully understand what happens with cryptocurrencies, a basic understanding of blockchain systems, as well as how it works and enables trust is essential. Before a more detailed and thorough definition is given, a straightforward way to understand blockchain technologies is that they are the solution to the issue of conducting data transactions without involving any third-party entities (Yli-Huumo et al. 2016). Blockchain is the underlying technology behind cryptocurrencies and has as core elements, complex cryptographic functions, linear and nonlinear data structures, peer-to-peer networks, and distributed consensus protocols. A more detailed definition is that blockchain is a distributed ledger with a consensus protocol which gets rid of centralized management controlling transactions thus decentralized, relying on a P2P network where anyone can participate (permissionless). When joining is restricted by the need of registration and verification of participants it is a permissioned blockchain. Each participant (also called node) within a blockchain network can access a copy of all previous (valid) transactions in the blockchain in a series of blocks. Each such block consists of firstly data dependent on that particular blockchain system, and second a hash for representing the current block and a hash to represent the previous block. The hashes serve as a digital fingerprint for each block and whenever a new transaction is processed, the hash is sent to participants to verify within the network. A consensus protocol, in simple wording, is when miners successfully solve and create a block, with the successful completion of the block each miner receives a certain amount of cryptocurrency tokens. Then the newly created block is sent to the rest of the network to be approved by comparing the hash of it with the hash of the previous block and lastly the blockchain is updated with the new block accordingly. The consensus protocol makes blockchain networks not only secure but immutable as well, since if the data of just a single block is altered then the hash changes and becomes invalid not only for the block altered but for all the following blocks as well and for the change to be accepted a very time and energy consuming process must take place called hash regeneration (Orcutt, 2018). It should be noted that protocols may differ depending on the blockchain application. Now that a thorough definition has been developed, a look at the main challenge of blockchain technology would be easier to understand. The huge problem of blockchain is scalability as huge storage and capacity infrastructure is necessary to save and validate millions of transactions in real time (Xie et al. 2018). The first application of blockchain technology was developed by Satoshi Nakamoto and released in early 2009, it is called Bitcoin and although the technology was not new or revolutionary the way it was used by not allowing double-spending was groundbreaking in allowing for the creation of digital assets (Orcutt, 2018).

Following, cryptography, the key factor of sales success in the combination of blockchain and cryptocurrencies. A simple definition could be given as, rights for writing and reading transaction records. As introduced by Peters and Panayi (2016), to classify the infrastructure of cryptocurrency systems there are four dimensions which are, “public” vs “private” and “permissioned” vs “permissionless”. In more detail, in public-permissionless systems every network participant has the ability to read transactions and write others to the ledger. In public-permissioned systems only authorized participants can write while in private-permissioned systems even reading is restricted solely to the participants authorized. The use of cryptography although has been highlighted and widely stated along with cryptocurrencies is nothing new and has been in use by banks for fiat currency long ago, therefore the term security should not be included in a definition of cryptocurrency. Moreover, the strong cryptographic and anonymous approach taken by creators of crypto tokens as well as advocates, does raise some concerns about anti-money laundering and law enforcement (Papamanthou et al. 2018).

Finally, an overview of a few models for trust analysis for cryptocurrency. Let us begin by clearly stating that trust as a term has never been formalized or quantified in the blockchain technology community and although multiple trustworthy facets of cryptocurrency systems exist the community collectively agrees that solving the inherent technical and non-technical issues in cryptocurrency platforms has the potential to lead towards a trustworthy, participatory, and inclusive crypto community (Rehman et al. 2019). With what said lets slightly graze the icebreaker of trust analysis models in blockchain cryptocurrency ecosystems. Starting off, with the model of Rehman, Salah, Damiani and Svetinovic (2019) which includes 7 basic features that all blockchain systems must provide to ensure a trustworthy platform. These are 1) trustless, preventing manipulation from centralized entities, 2) decentralization, 3) distributed ledger technology, 4) tamper-proof environment 5) security and privacy, 6) consensus mechanism and 7) faster transactions (Figure 1). Another important analysis model is that of Suhail (2022) which analyzes over 7 external factors that influence trust which are 1) presence of other systems, 2) risks perceived, 3) benefits perceived, 4) subject matter expertise, 5) reputation, 6) clarity, 7) support by major players. Suhail also analyzes 11 internal factors who go as follows, 1) performance, 2) portability, 3) usability, 4) dependability, 5) identity, 6) security, 7) privacy, 8) decentralization, 9) reputation, 10) clarity of policy and rules, 11) support (figure 2). It is also mentioned that technical factors have less influence on trust with decentralization being the top systematic reason for the increase of trust because it reduces the impact of the external factors. However, more aspects of trust were identified and considered under further investigation. Finally, the last trust model is that of Khalifa, Madjid and Svetinovic (2019) which tackles the problem by taxonomy of trust within the System Requirements. The system requirement is divided into 2 categories, functional or non-functional, focusing on the latter with it later being split into another two categories, constrains and properties under properties another 8 categories are split including privacy, security, portability and more (figure 3). It is also key to highlight that an application which is blockchain-based acquires consistency by accepting or rejecting blocks when they do not comply with the rules (Smith, 2017). With a quick look at these 3 models, it is easily understandable that

researchers share the same concerns and problems, with not only cryptocurrencies and cryptocurrency systems but with blockchain technologies in general.

In conclusion, cryptocurrency is a volatile, unregulated space which still lacks stableness, and the stakeholder's knowledge is limited to prosper. Although it is easy to fall victim to fake crypto millionaire gurus that will help you become rich, research and skillful knowledge is necessary when consolidating with money and online platforms. The takeover of cryptocurrencies and digital assets, although visible, still lacks fundamental elements and qualities, more importantly on getting trusted from stakeholders. After all, whatever potential, and revolutionary features a technology provides, if a stakeholder does not have sufficient trust in the technology there is little to no chance, they will use it even less rely on it for basic needs.

Figure 1:

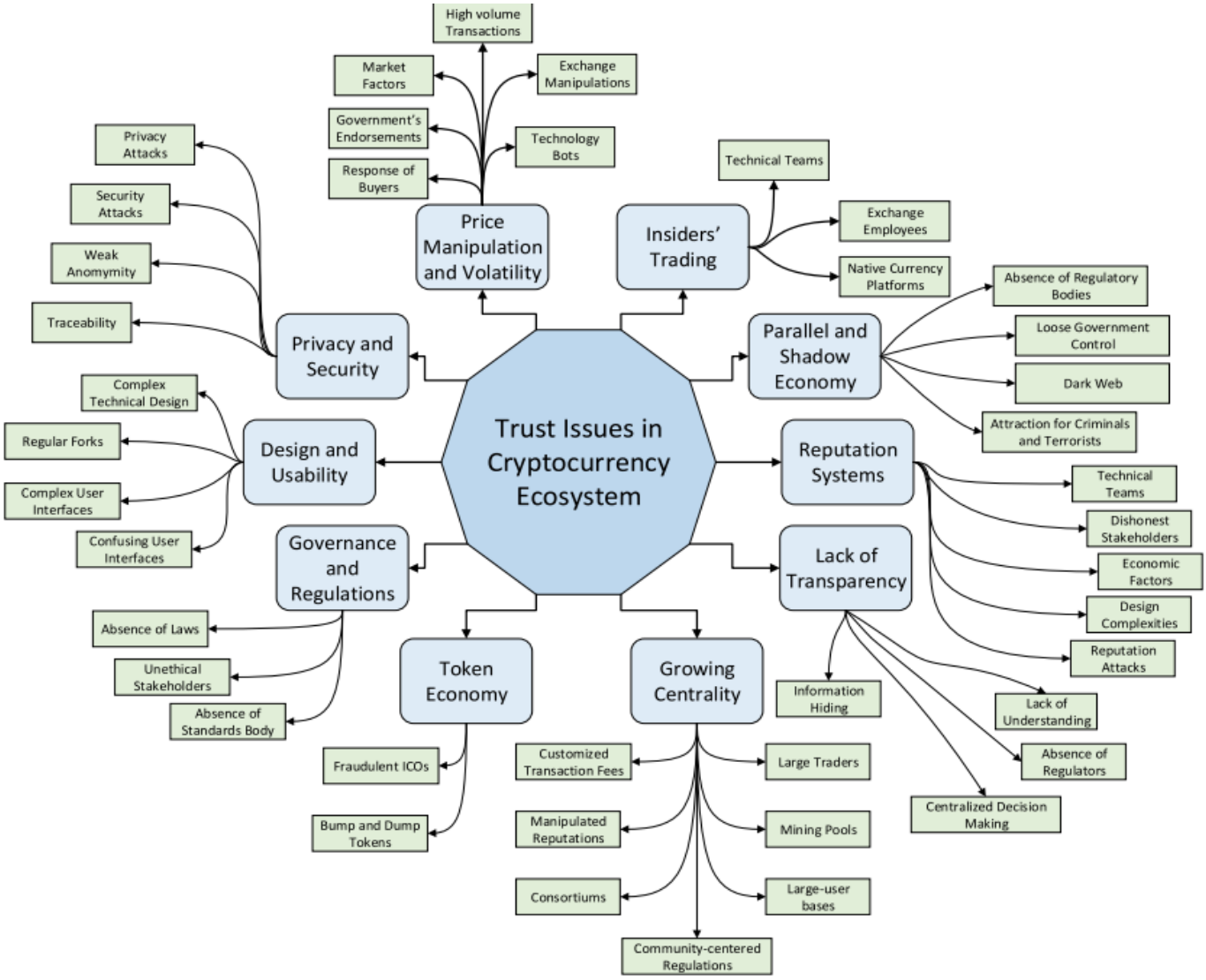
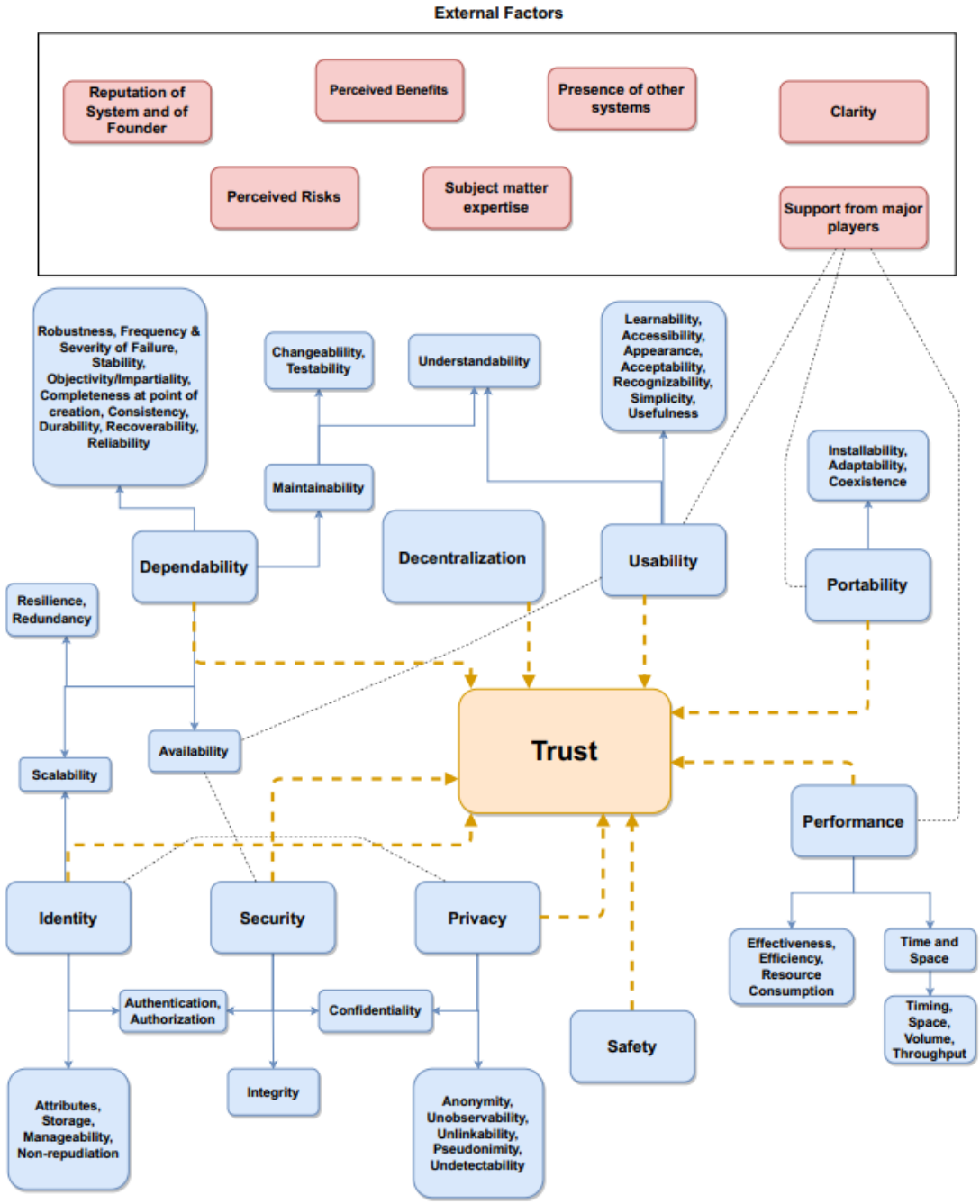
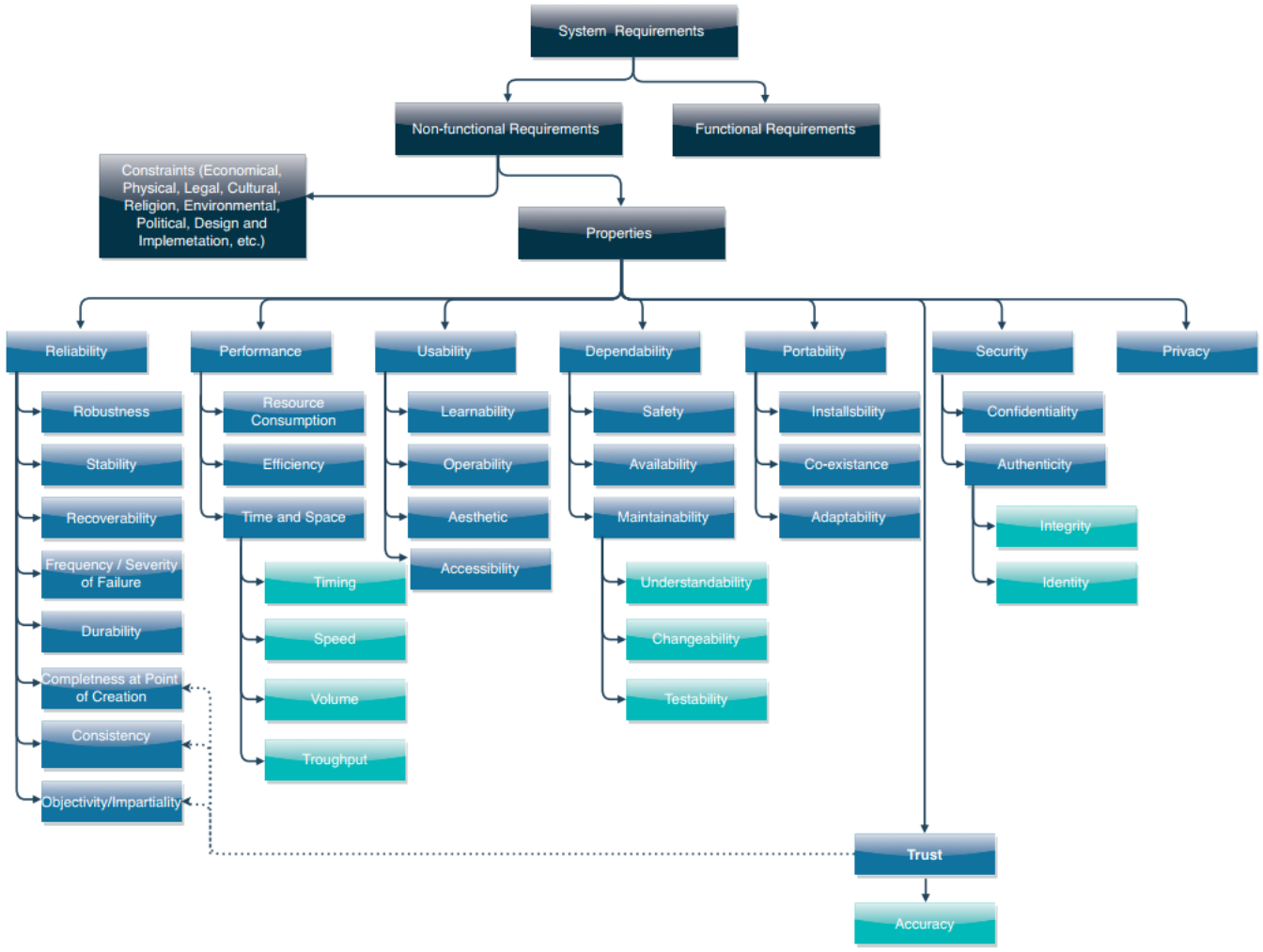

Trust Issues in Cryptocurrency Ecosystem
Price Manipulation and Volatility
High volume Transactions
Market Factors
Exchange Manipulations
Government's Endorsements
Technology Bots
Response of Buyers
Insiders' Trading
Technical Teams
Exchange Employees
Native Currency Platforms
Parallel and Shadow Economy
Absence of Regulatory Bodies
Loose Government Control
Dark Web
Attraction for Criminals and Terrorists
Reputation Systems
Technical Teams
Dishonest Stakeholders
Economic Factors
Design Complexities
Reputation Attacks
Lack of Transparency
Information Hiding
Lack of Understanding
Absence of Regulators
Centralized Decision Making
Growing Centrality
Customized Transaction Fees
Large Traders
Manipulated Reputations
Mining Pools
Consortiums
Large-user bases
Community-centered Regulations
Token Economy
Fraudulent ICOs
Bump and Dump Tokens
Governance and Regulations
Absence of Laws
Unethical Stakeholders
Absence of Standards Body
Design and Usability
Complex Technical Design
Regular Forks
Complex User Interfaces
Confusing User Interfaces
Privacy and Security
Privacy Attacks
Security Attacks
Weak Anomymity
Traceability

Figure 2:



The solid arrows represent requirement(s) type; dotted lines represent relationship between them; dashed arrows represent contribution of requirement type to trust.

Figure 3:


System Requirements
Non-functional Requirements
Functional Requirements
Constraints (Economical, Physical, Legal, Cultural, Religion, Environmental, Political, Design and Implemetation, etc.)
Properties
Reliability
Performance
Usability
Dependability
Portability
Security
Privacy
Robustness
Stability
Recoverability
Frequency / Severity of Failure
Durability
Completness at Point of Creation
Consistency
Objectivity/Impartiality
Resource Consumption
Efficiency
Time and Space
Timing
Speed
Volume
Troughput
Learnability
Operability
Aesthetic
Accessibility
Safety
Availability
Maintainability
Understandability
Changeability
Testability
Installsbility
Co-existance
Adaptability
Confidentiality
Authenticity
Integrity
Identity
Trust
Accuracy

References:

- Pernice, Ingolf Gunnar Anton and Scott, Brett, Cryptocurrency (May 20, 2021). Internet Policy Review, Glossary of decentralised technosocial systems, Volume 10, Issue 2
- N. Elsokkary, M. Habib ur Rehman, S. Suhail, H. Kaindl and D. Svetinovic, "Trust Evaluation of Blockchain-Based Cryptocurrencies: The Cases of Bitcoin and Diem," 2022 International Balkan Conference on Communications and Networking (BalkanCom), Sarajevo, Bosnia and Herzegovina, 2022, pp. 73-77
- D. Khalifa, N. A. Madjid and D. Svetinovic, "Trust Requirements in Blockchain Systems: A Preliminary Study," 2019 Sixth International Conference on Software Defined Systems (SDS), Rome, Italy, 2019, pp. 310-313
- B. Craggs and A. Rashid, "Trust Beyond Computation Alone: Human Aspects of Trust in Blockchain Technologies," 2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Society (ICSE-SEIS), Montreal, QC, Canada, 2019, pp. 21-30
- Bucko, Jozef & Palová, Dana & Vejačka, Martin. (2015). Security and Trust in Cryptocurrencies.
- Arli, D., van Esch, P., Bakpayev, M. and Laurence, A. (2021), "Do consumers really trust cryptocurrencies?", Marketing Intelligence & Planning, Vol. 39 No. 1, pp. 74-90.
- Dirk Bullmann, Jonas Klemm, and Andrea Pinna. “In search for stability in crypto-assets: are stablecoins the solution?” In: ECB Occasional Paper 230 (2019)
- Jeremy Clark, Didem Demirag, and Seyedehmahsa Moosavi. “Demystifying Stablecoins: Cryptography meets monetary policy”. In: Queue 18.1 (2020), pp. 39–60.
- Valeria Ferrari. “The regulation of crypto-assets in the EU–investment and payment tokens under the radar”. In: Maastricht Journal of European and Comparative Law 27.3 (2020), pp. 325–342
- Daniel Genkin, Dimitrios Papadopoulos, and Charalampos Papamanthou. “Privacy in decentralized cryptocurrencies”. In: Communications of the ACM 61.6 (2018), pp. 78–88
- Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system [White Paper]. 2008.
- Satoshi Nakamoto. Bitcoin open source implementation of P2P currency [Forum post]. 2008.
- Gareth W Peters and Efstathios Panayi. “Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money”. In: Banking beyond banks and money. Springer, 2016, pp. 239–278
- Elina L Sidorenko. “Stablecoin as a new financial instrument”. In: International Scientific Conference “Digital Transformation of the Economy: Challenges, Trends, New Opportunities”. Springer. 2019, pp. 630–638

- Giannis Tziakouris. “Cryptocurrencies—a forensic challenge or opportunity for law enforcement? an interpol perspective”. In: IEEE Security & Privacy 16.4 (2018), pp. 92–94
- X. Li and C. A. Wang, “The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin,” Decis. Support Syst., vol. 95, pp. 49–60, 2017
- Mike Orcutt. Blockchain: What is it? MIT Technology Review, page 18–25, 5 2018
- Z Xie, S Dai, H-N Chen, and X Wang. Blockchain challenges and opportunities: a survey. Technical Report 4, 2018
- Alex Zarifis, Leonidas Efthymiou, Xusen Cheng, and Salomi Demetriou. Consumer Trust in Digital Currency Enabled Transactions. pages 241–254. 2014