Cover Page

1. Project proposal title (up to 200 characters): **Advanced Artificial Intelligence Techniques for Analysis and Design of System Components Based on Trustworthy BlockChain Technology**
2. Acronym (up to 20 characters in English or Serbian as used throughout the Project Proposal): **AI4TrustBC**
3. Participating SROs acronyms (up to 20 characters): **MISANU, FTN**
4. Subprogram (Fundamental or Applied Research): **Fundamental Research**
5. Research field of the Project: **Knowledge reasoning**
6. Participating Scientific and Research Organizations (SROs) and their acronyms: **Mathematical Institute of the Serbian Academy of Sciences and Arts (MISANU) and Faculty of technical Sciences, University of Novi Sad (FTN)**
7. Principal Investigator (PI): **Tatjana Davidović**
8. Abstract (up to 2000 characters):

BlockChain (BC) is a distributed data storage structure maintained without any third party of absolute trust. Over the last ten years, since its first implementation in cryptocurrency, BC technology has been applied to a wide range of applications in IoT, insurance, healthcare, smart contracts, finance, digital identity, voting, notary, among others. BC is a public ledger where data are added simultaneously and remain immutable. Verification of data without trusted third parties is realized by consensus protocols and provides trustworthiness of BC. Artificial Intelligence (AI) and BC are proven to be quite a powerful combination, improving virtually every industry in which they are implemented. The goal of this project is to contribute to the application of AI to the BC technology domain in two basic ways: knowledge reasoning techniques are to be used to analyze consistency of consensus algorithms for BC; AI techniques are to be employed for the analysis of anonymous data in order to evaluate robustness of privacy protection in BC. The expected results of this project are: to develop formal logic based knowledge reasoning techniques for analyzing the BC protocol; to develop knowledge reasoning techniques and formal methods for privacy management based on trustworthy BC technology; to develop new Proof-of-Work tasks based on hard optimization problems and examine their performance; to develop metaheuristic-based tools for the analysis of system security; to employ AI techniques to evaluate security of certain BC consensus protocols; to employ AI techniques to evaluate privacy evaluation of certain BC ledgers. In general, the project as a whole is meant to advance the mutual applicability AI to BC and BC to AI. The project impact is ranging from foundational to highly practical and from individual privacy protection to the society as a whole, where privacy is one of the key issues.

9. Total requested budget in EUR: **176,123.98**

Project Description - Part A

1. Excellence

BlockChain (BC) (introduced in the white paper by Nakamoto, 2008) is a specially designed data storage structure, maintained without any third party of absolute trust. The first BC implementation was related to the financial domain - performing transactions with Bitcoin cryptocurrency. BC could be regarded as a public ledger where all data (referred to as "committed transactions") are stored in a list of blocks (Zheng et al, 2017). New data (organized in blocks) from different domains (cryptocurrency/finance, digital identity, voting, notary, smart contracts, IoT, insurance, healthcare, etc.) are allowed to be added simultaneously. Only blocks verified by the agreement between a given number of agents (entities, nodes) could be added to the chain and they cannot be changed anymore (they remain immutable). The core property of BC is that validation of the blocks to be added is performed without involving a so-called "third party of absolute trust", while the immutability and security is ensured by cryptology techniques. Verification of data without "trusted third parties" is realized by the so-called consensus protocols most of which are based on cryptology techniques.

BC is basically a distributed system (distributed ledger) that can be centralized or decentralized. It means that this ledger is spread across the network, and each of the network partners holds a copy of the complete ledger. In this distributed system nodes can be defined as individual players, and messages can be sent and received between them. As having memory and processor nodes, BC can become a subject of dishonest user attitude, being damaged or become dangerous itself. Therefore, the problem of distributed consensus in the network without trust arose.

The BC consensus protocol is characterized by the following properties:

- It is managed autonomously, without third authority.
- It removes the possibility of infinite reproducibility from a digital asset, i.e., it confirms that each unit of value was transferred only once, solving the long-standing problem of resource wasting by doubling data.
- It can assign title rights to agents by properly setting the exchange agreement between the agents that will cooperate to outpace attackers.

The consensus algorithm is responsible for maintaining the integrity and security of the whole BC based system. Any BC system has a distributed structure and does not rely on a central authority. The consensus protocol is employed in order to provide the validity of transactions. In other words, validity of a transaction should become common knowledge of all agents. Therefore, one of the crucial properties in the BC consensus protocol is to guarantee that in every execution step consensus is achieved and that all transactions occur in a trustful way. Consequently, the reliability and security of the consensus protocols appear as the top importance issues. A lot of consensus protocols are based on certain cryptographic puzzles related to the inversion of one-way functions noting that beside a traditional hash function, other one-way functions could be employed particularly taking into account advances in this topic (see, as an illustration Mihaljevic, 2019). When the consensus protocol is based on solving a cryptographic puzzle, it could be performed by spending certain computational resources, i.e., performing some work, and these protocols are denoted as Proof-of-Work ones.

When the consensus protocol is based on the Proof-of-Work paradigm, the basic steps of the protocol are as follows:

1. New transactions are broadcast to all agents.
2. Each agent collects a subset of new transactions into a block.
3. To verify its block, the agent has to solve a difficult Proof-of-Work task for that block.
4. When an agent solves a Proof-of-Work, it broadcasts the block and the solution to all agents.
5. Agents verify a Proof-of-Work, validity of transactions in the block, and their uniqueness and accept the block if all verifications passed. Otherwise, block is rejected.
6. The accepted block is added to the end of chain, together with the hash that would be used to verify the upcoming blocks.

It could happen that two agents broadcast different versions of the next block simultaneously, and branching occurs in the chain. The longest chain, i.e., the one containing the most Proofs-of-Work, is favored, it is considered to be the correct one and all agents will keep working on extending it.

The main task in designing and implementing BC is to ensure the consistency of distributed data, i.e., that each copy of a data contains the same value. Another important task is to disable the analysis and knowledge discovery of recorded data that would raise the privacy issues and compromise the entire system. Consequently, the evaluation of the system security is one of the essential tasks that should engage advanced approaches and techniques, which, on the other hand, should provide basis for the construction of safer components of the BC based systems.

Artificial Intelligence (AI) and BC are proven to be quite a powerful combination, improving virtually every industry in which they're implemented. Recently, it has been acknowledged that artificial intelligence techniques can be of significant importance for the evaluation of components and entire BC systems (Dillenberger et al, 2020; Marinković et al, 2019; Salah et al, 2019; Tanwar et al, 2020; Wang et al, 2020). AI can effectively mine through a huge dataset to create newer scenarios and discover patterns based on data behavior. Therefore, the goal of this project is to provide contribution to the application of artificial intelligence in the BC technology domain:

- **Knowledge reasoning techniques can be used to analyze consistency of consensus algorithms for BC.**
- **Employment of AI techniques for the analysis of anonymous data in order to evaluate robustness of the privacy protection in certain BC ledgers.**

The project would deal with the open problems that have arisen due to the rapid technological breakdown and would explore new artificial intelligence techniques for presenting and discovering knowledge, managing privacy, ensuring consistency and reliability of modern BC technology. Within this project we propose to develop and use knowledge reasoning techniques based on formal methods, non-classical logics, and metaheurists (the fields of expertise of the project team members) to deal with the above mentioned challenges. The main research goal would encompass the implementation and performance examination of the BC systems with incorporated the above mentioned artificial intelligence techniques and their comparison with classical BC implementations.

The structure of BC and AI involvement are illustrated in Fig. 1.

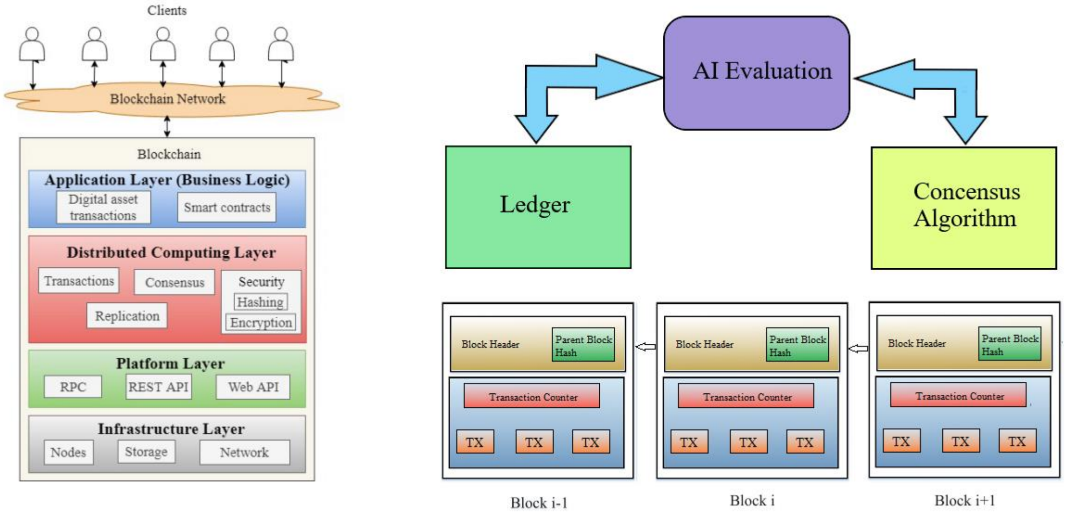

Fig. 1

1.1. Objectives

- To develop formal logic based knowledge reasoning techniques for analyzing the BC protocol;
- to develop knowledge reasoning techniques and formal methods for privacy management based on trustworthy BC technology;
- to develop new Proof-of-Work tasks based on hard optimization problems and examine their performance;
- to develop metaheuristic-based tools for the analysis of system security;
- to employ AI techniques to evaluate security of certain BC consensus protocols;
- to employ AI techniques to evaluate privacy evaluation of certain BC ledgers.

1.2. Concept and methodology

As we already mentioned, formal methods, non-classical logics, and metaheurists will be used to model, analyze and design various components of BC technology. Here we describe these concepts and methodologies concerning the project issues in more detail.

1. Formal Models for privacy management

Linked data recently equipped with a type system (Jaksic et al., 2017) can statically detect run-time errors due to privacy violations. Resources (URIs) are denoted by names from a specified set. Data are parallel composition of triples of names (describing links between resources). Processes are ´-calculus processes, without input and output capabilities, and with introduced capabilities that describe the interaction between processes and data. Networks are parallel composition of user names enclosing data and processes. In order to enable each owner of data to control privacy of the data, we assign a query to each user name and also a query to each data triple. This is a simple yet sufficiently powerful type assignment system which, together with the introduced query order, is able to statically check if a network is well behaved. We plan to extend this pioneering work with focus to all three privacy violation groups, data collection, processing a distribution (Solove, 2006) in linked open data setting. Behavioral types and session types, which extend data types by describing also the structured behavior of programs, are a widely studied approach to the enforcement of correctness properties in communicating systems and to the analysis of security protocols (Bartoletti et al., 2015).

Recent results of formal models for management of privacy in the domain of linked data (Jaksic et al., 2017), access control (Dezani et al., 2008) and multiparty conversations (Ghilezan et al, 2016; Bartolettiet al. 2015) will be further developed to BC technology. We will build on our experience on behavioral types and contract theory as well as on a novel approach formalizing the actor model as a type discipline. We will test the designed type disciplines in two approaches to concurrency ´-calculus and actor model against privacy violation and find the most appropriate for each one of the three groups (collection, processing and distribution). We plan to examine privacy management in this setting and extend the theory accordingly using all available type-theoretic methods (Dezani et al., 2008; Ghilezan et al., 2016; Kouzapas and Philippou, 2018).

2. Randomness and probabilistic reasoning in privacy menagement

Reasoning with uncertainty has gained an important role in computer science, artificial intelligence and cognitive science. These applications urge for development of formal models which capture reasoning of probabilistic features. The group members have a recognised expertise in probabilistic logic (Ognjanovic et al., 2016). Recent work (Ghilezan et al., 2018) develops a formal model for reasoning about probabilities of type systems with focus to lambda terms with intersection types: its syntax, Kripke-style semantics and axiomatic system. The main results are the corresponding soundness and strong completeness, which relay on two key facts: the completeness of lambda calculus with respect to the filter lambda model and the existence of the maximal consistent extension of a consistent set. We plan to combine this work with secrecy for multiagents and extend it to privacy management.

General Data Protection Regulation (GDPR) aims to give control to the citizens regarding the use of their personal data by businesses and enterprises, by defining requirements for processing this kind of data. Specifically, the GDPR requires that any business process must implement data protection by design and by default. One principled approach to achieve this in the context of data mining is the mechanism of differential privacy. With differential privacy, there is a guarantee that individual records of a dataset cannot be learned even when an arbitrary outside information is provided. This is achieved by introducing randomness, by the data curator, into response to queries, posed by machine learning algorithms to the database. The size of the randomness is controlled by the, so called, epsilon factor, or the privacy cost that trades-off the level of achieved privacy with performance of the machine learning algorithm in question. Depending on a given machine learning algorithm, there are many ways in which one can implement differential privacy. In practice, the latter translates into the question at what level of the algorithm and what kind of queries will be perturbed by noise.

3. Non-classical logic for analysis of BC protocols

Representation of and reasoning about knowledge are two of the main fields of AI that focus on:

- designing of representations that capture information about the world and
- developing methodologies that can be used to solve complex problems.

Mathematical logic provides some key enabling tools to describe and work with knowledge. Expressive power of non-classical logics (epistemic, temporal, probabilistic, etc.) allows modelling properties of real-world situations and reasoning about (possibly incomplete and/or uncertain) knowledge, its changes and resulting actions. Protocols can be seen as formalizations of processes that perform actions and change states of systems. A well founded approach to defining and analyzing messagepassingï based distributed and nondeterministic protocols is based on non-classical logics and Kripke-like modal semantics with possible worlds equipped with probability measures and accessibility relations concerning epistemic and temporal operators (see Halpern, 2017). To the best of our knowledge, the first paper in the literature which provides formal logical analysis of the BC protocol was by MarinkoviÍ et al, 2019 (one of the authors is a member of the proposed project team). In this paper, the authors have proposed a strongly complete Hilbert-style axiomatization of a temporal epistemic logic with respect to Kripke-like semantics in which the set of active agents needs not be rigid, i.e., an agent may alternately become active and inactive. The formal language, besides Boolean operators, included the temporal operators Next and Until, and the epistemic operators for Knowledge and Common knowledge. The proved statements about the logic enabled to define a theory (a set of proper formulas) which axiomatized the class of models describing the BC protocol. It was possible to investigate which assumptions about the BC protocol (i.e., which formulas) entail particular properties of the protocol. The main result was that the proposed theory which corresponds to the BC protocol is consistent, and that the theory implies that active agents, after a fixed number of rounds, have an agreement and also that this agreement is their common knowledge (i.e., every agent knows that every agent knows é etc.). The assumptions that guarantee obtaining a consensus among the agents on the next block to be added to the ledger are determined. The main shortage of the approach is that the paper does not consider the probabilistic nature of the BC protocol, and the main constraint of the paper is the assumption that events with high probability are necessary (i.e., they always happen).

However, as probabilistic nature is one of the main characteristics of the BC protocol, the presented results give only a rough approximation of the BC protocol behavior. So, one of the goals of the project is to extend the previous work and to develop a formal framework which will take more realistically into account probabilistic aspects of the BC protocol. More precisely:

- a formal language (containing the probabilistic, epistemic and temporal operators) will be defined,
- a Kripke-like semantics (i.e., a class of models) will be defined,
- an axiom system will be proposed,
- it will be proved that the axiomatization is sound and strongly complete wrt. the considered semantics,
- decidability of the logic will be analyzed,
- a theory (set of proper axioms) will be developed to describe the BC protocol, and
- this theory will be used to analyze properties of the BC protocol.

Temporal and epistemic logics are broadly analyzed in the literature. The ability to describe properties of programs using the future-time linear discrete temporal logic (LTL) focused research on it, while to characterize properties of knowledge authors used axiomatizations based on modal systems S5 and KD45 (e.g., see Halpern et al, 2004.). A bridge which connects semantics and syntax can be established by the soundness and completeness theorems. The usual forms of those theorems are:

- the weak (or simple) completeness: a formula is consistent iff it is satisfiable (i.e., a formula is valid iff it is provable), or
- the strong (or extended) completeness: a set of formulas is consistent iff it is satisfiable (a formula is a syntactical consequence of a set of formulas iff it is a semantical consequence of that set).

While the former statement follows trivially from the latter, the opposite direction does not. In classical propositional and first-order logics these theorems are equivalent, thanks to a significant property called compactness: a set of formulas is satisfiable iff every finite subset of it is satisfiable. The main technical challenge in axiomatizing probability, temporal and epistemic logic and their combination lies in the fact that for these logics the property of compactness does not hold. Thus, we propose an approach that solves that issue by relying on infiniteness which has proved to be a powerful tool in this endeavor. Some basic efforts in that direction are presented in the book by OgnjanoviÍ et al., 2016 (the first author is a member of the proposed project team). We will use tools as weak as possible, i.e., to limit the use of infinitary means limiting ourselves to use countable object languages and finite formulas, while only proofs are allowed to be infinite. Another important problem which will be addressed is related to decidability. We will develop an efficient decision procedure which combines reduction to finitely representable discrete linear time models, filtration for modal logics and solving of linear systems that represent probabilistic constraints.

4. Metaheuristics for designing and analysis of BC consensus protocols

Metaheuristics are modern optimization methods, usually based on well-known biological processes (for example the swarm intelligence), that have recently been shown extremely efficient for data classification, feature selection and knowledge extraction out of big databases. Within the BC systems, metaheuristics were used for modeling and implementing data verification procedures, and our investigations would extend these results as well as include considering of other system components.

In a large number of scenarios we face particular instantiations of the following general problem: All updates of a huge database should be verified before becoming effective. A generic approaches for performing the verification is the centralized one where a trusted party check and verifies all the updates. The main problem with this approach is necessity of existence a third trusted party as well as the generic problem of the single point of failure. Recently, as an alternative approach, the BC paradigm has been proposed within the Bitcoin proposal, where the verification is performed in a distributed manner without requirement for the third trusted party as the verification arbiter. The removal of the third trusted party and the distributed verification approach requires an appropriate technique for achieving the verification decision: For this purpose the BC-based verification employs the so called consensus protocol. This consensus protocol appears as a system overhead. We could say that the escape from the centralized verification paradigm should be paid by the overhead related to the required BC consensus protocol. The overheads implied by the employed consents protocol could be very large and it is an open research issue to construct dedicated consensus algorithms in order to minimize the overheads in a system based on BC technology.

Traditional BC consensus protocols (see: Salah et al, 2019):
1) Proof-of-Work (PoW)
2) Proof-of-Stake (PoS)
3) Byzantine Fault Tolerance (BFT)
4) Proof-of-Activity (PoAc)
5) Proof-of-Burn (PoB)
6) Proof-of-Elapsed-Time (PoET)
7) Proof-of-Capacity (PoC)
8) Proof-of-Authority (PoA)
9) Proof-of-Importance (PoI)

For example, let public key cryptography with the PoW mechanism is used to provide a safe, controlled and decentralized method for managing the consistency of BlokChain system. In order to add new blocks to BC, agents must compete to find the right public key, the number that is less than the given target. The difficulty in finding the right value is also sometimes called a cryptographic puzzle (Syafruddin, et al, 2019). BC security generally comes from such a cryptographic puzzle used for adding (mining) new blocks into the system. However, this consensus algorithm was facing some serious problems in wasting too much electrical energy because it requires a lot of computer calculations (Taylor, 2018). In (Syafruddin, et al, 2019) it is proposed to change PoW mechanism in such a way that, instead of hash function (the usual cryptographic puzzle), agents need to solve a hard combinatorial optimization problem, namely Traveling Salesperson Problem, TSP. A suboptimal solution of a large TSP instance is provided (as a target value) with each new block to be added to BC. To obtain a representative target value, Particle Swarm Optimization (PSO) metaheuristic was used. This concept is new and slightly explored, and therefore, opens a whole new research topic involving different optimization problems (satisfiability, set partitioning, packing and scheduling, etc.) as well as various metaheuristic methods, especially Variable neighborhood Search, VNS (MladenoviÍ and Hansen, 1997; Hansen et al, 2017) and Bee Colony Optimization, BCO (TeodoroviÍ and Dell'Orco, 2005, DavidoviÍ, 2015). The realized BC systems could be compared with the ones using classical PoW mechanism and Proof-of-Collatz Conjecture (PCC), proposed in (Aljassas and Sasi, 2019).

5. Metaheuristics for clustering in BC systems

Motivations for clustering of BC data can be classified into three following categories: 1. Fraud Detection and Law Enforcement, 2. Systems Insights, and 3. Anonymity and Traceability.

1. By design, all transfer of currency is publicly and persistently recorded, so it would seem that thieves should be exposed when they try to cash out by exchanging the cryptocurrency for conventional fiat currency. A related objective is tracing the flow of finances among people and organizations engaged in criminal activities that are using Bitcoin for payments, e.g., the WannaCry ransomware attack (Collins, 2017). However, such detection is difficult in practice because there is no requirement for Bitcoin addresses to be registered in any manner, at least until a transaction with a conventional currency exchange is required. Further, there is no practical limit on the number of addresses that a person or organization may generate, so it is easy to create complex chains of transfers that obfuscate the origin of funds. Nevertheless, a careful study of Bitcoin addresses and transactions, along with some external information, such as accidentally or casually revealed connections between Bitcoin addresses and entities, can be used to uncover many such schemes.
2. The global, distributed, peer-to-peer system that maintains BC is an intriguing and impressive artifact in its own right, worthy of study for computer science and, in particular, systems insights (Awan and Cortesi 2017, Pongnumkul et al, 2017). More specifically, by studying the frequency, value, and other characteristics of transactions, and other properties of the underlying system, and designers of not only BC systems, but other large distributed systems as well, are likely to derive valuable insights.
3. Bitcoin provides a form of anonymity that has been called pseudoanonymity: On one hand, every Bitcoin transaction is fully public, and permanent, and thus practically impossible to conceal. On the other, the only form of identity required to transact in Bitcoin is a randomly generated address, which on its own lacks any identifying information. While this anonymity can and has been used for nefarious purposes, it is also useful for legitimate privacy reasons. However, as noted in the original Bitcoin paper (Nakamoto, 2008) itself, the anonymity of a Bitcoin addressôs owner may be compromised by patterns in transactions. Studying clustering and related methods

for analyzing BC allows the community to better understand the limitations of the anonymity provided by Bitcoin and other BCs (Ober et al, 2013).

The main ingredients in BC clustering are as follows: Modeling of data, Decision what will be clustered, and Evaluating clustering.

Modeling data in BC

The same base BC dataset may be modeled and abstracted in different ways for the purposes of clustering. For example, Bitcoin transaction data may be modeled as a graph with transactions represented by vertices and input-to-output references modeled by directed (reverse) edges, but also as a graph with Bitcoin addresses as vertices and payments as edges. In addition, models may include the other components of the BC infrastructure, such as transactions, the blocks themselves, and the hosts in the peer-to-peer network (represented by addresses, owners, nodes).

Clustering

The first approach is based on applying mostly conventional, well-studied clustering algorithms (e.g., k-means) and robust implementations to feature-vectors extracted from BC datasets (Ghahramani, 2004, Jain et al, 1999, Kohonen, 2013, Zhang, 2007). The key tasks in this case are determining the set of features to use, extracting them effectively from the underlying data, and transforming them (e.g., scaling, normalization) to improve clustering. The associated challenge of scaling clustering methods to the size and throughput of BC datasets is an important one as well, but one that may be addressed using well-developed prior work on clustering large datasets in general.

The second approach is based on a more direct utilization of the particular characteristics of BC data, e.g., co-occurrence of transaction inputs, or other temporal patterns (Epishkina and Zapechnikov, 2017) and their associated semantics, e.g., identical or closely related owners. The key tasks in this case are determining which semantics, assumptions, and heuristics to use for the purpose of forming clusters, and designing algorithms tailored to those that are capable of efficiently operating on the large datasets involved.

Evaluating clustering

The most direct methods for evaluating the results of a clustering algorithm, and related indices (such as *purity* and *entropy*), are based on determining how well the algorithm detects clusters that have been determined by some other method, typically with human input. For BC data, such an external evaluation method is of very limited effectiveness due to the scarcity of such tagged and well studied datasets. The volume of data, as well as other characteristics, mean that it is impracticable to rely on the availability of such test data in the near future as well. It is therefore necessary to use methods that do not rely on human-studied datasets but, instead, use some other intrinsic characteristics of the input data and output clusters, i.e., an internal method. Majority of these methods are distance-based and selecting proper distance is one of the most important tasks.

Generally, there are two variants of clustering: supervised clustering and unsupervised clustering. In the supervised clustering the goal is to learn a model from labeled data sets. The learned model is then applied to an unlabeled (unseen) test set and the method is validated based on how successful it was in dividing test data into proper (correct) classes. The disadvantage of supervised learning techniques is that they are limited to learning from labeled datasets which are often expensive, time consuming, or difficult to generate. If the available labeled dataset is too small and does not represent the true variance of the data space then generalization performance may be poor. Most of supervised clustering methods are based on artificial neural networks (ANN) and support-vector machines (SVM). In the unsupervised clustering the goal is to develop method which can cluster (divide) arbitrary dataset (from the corresponding family), usually by minimizing (maximizing) value of selected evaluation function. Therefore, the unsupervised clustering can be considered as combinatorial optimization problem, and because of that any of metaheuristic method can be applied for solving. Different metaheuristics are successfully applied to similar problems: p-median, p-center, clique partitioning problem (Brimberg et al, 2017), etc. Especially, we think that variable neighborhood search, Primal-Dual variable neighborhood search (Brimberg et al, 2009) and bee colony optimization (Davidovic et al, 2018) can be applied for unsupervised clustering.

During the project we will analyze BC data and decide how to model these data (as vectors of extracted features, or as vertices of directed graph with arcs describing relation between vertices). After that, we will implement methods for clustering based on the above mentioned metaheuristics. Implemented methods will be executed on selected BC data, and obtained clusters will be further analyzed.

References (the names of the project team members are in bold):

1. H. M. A. Aljassas and S. Sasi, "Performance Evaluation of Proof-of-Work and Collatz Conjecture Consensus Algorithms," *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, Riyadh, Saudi Arabia, 2019, pp. 1-6.
   doi: 10.1109/CAIS.2019.8769514

2. M.K. Awan, A. Cortesi, Blockchain transaction analysis using dominant sets, in Computer Information Systems and Industrial Management, ed. by K. Saeed, W. Homenda, R. Chaki. Springer, Cham (2017), pp. 229ï 239.

3. M. Bartoletti, I. Castellani, Pierre-Malo Denielou, M. Dezani-Ciancaglini, **S. Ghilezan**, J. Pantovic, Jo. A. Perez, P. Thiemann, B. Toninho, H. Torres Vieira: Combining behavioural types with security analysis, Journal of Logical and Algebraic Methods in Programming 84: 763ï 780 (2015).

4. J. Berman, D. Mulligan: Privacy in the digital age: Work in progress. Nova L. Rev. 23, 551 (1998).

5. J. Brimberg, S. Janicijevic, N. Mladenovic, **D. Urošević**, Solving the clique partitioning problem as a maximally diverse grouping problem, Optimization letters, 11, 1123-1135, 2017.

6. J. Brimberg, P. Hansen, N, Mladenoviĺ, **D. Urošević**, Solving large p-median clustering problems by primal-dual variable neighborhood search, Data Mining and Knowledge Discovery, 19, 351-375, 2009.

7. K. Collins, Inside the digital heist that terrorized the worldð and only made $100k. Quartz (2017). https://qz.com/985093/inside-the-digital-heist-that-terrorized-the-world-andmade-less-than-100k/

8. **T. Davidović**, Bee Colony Optimization: Recent Developments and Applications, (plenary talk), Proc. Balkan Conference on Operational Research, BALCOR 2015, Constanta, Romania, Sept. 9-12, 2015. Mircea cel Batran Naval Academy Scientific Bulletin, Volume XVIII, Issue 2, Dec. 2015, pp. 225-235.

9. **T. Davidović**, N. Gliġoviĺ, M. Raġkoviĺ, Bee Colony Optimization for Clustering Incomplete Data, *Proc. The 7th International Conference on Optimization Problems and Their Applications*, OPTA 2018, Omsk, Russia, July 08-14, 2018, In: S. Belim et al. (eds.): Proceedings of the School-Seminar on Optimization Problems and their Applications (OPTA-SCL 2018), CEUR Workshop Proceedings, 2018, pp. 94-108.

10. P. De Filippi: The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies. Journal of Peer Production, Issue n.7 (2016).

11. M. Dezani-Ciancaglini, **S. Ghilezan**, J. Pantoviĺ, D. Varacca: Security types for dynamic web data, Theoretical Computer Science 402 (2-3): 156-171 (2008).

12. C. Dwork: Differential Privacy: A Survey of Results. TAMCS 2008, Lecture Notes in Computer Science 4978: 1ï 19 (2008).

13. A. Epishkina, S. Zapechnikov, Discovering and clustering hidden time patterns in blockchain ledger, in First International Early Research Career Enhancement School on Biologically Inspired Cognitive Architectures (2017)

14. Z. Ghahramani, Unsupervised learning, in Advanced Lectures on Machine Learning, ed. by O. Bousquet, U. von Luxburg, G. Rätsch. Lecture Notes in Computer Science, vol. 3176, chap. 5 (Springer, Berlin, 2004), pp. 72ï 112.

15. **S. Ghilezan**, J. Ivetic, S. Kasterovic, **Z. Ognjanovic**, N. Savic: Probabilistic reasoning about simply typed lambda terms, LFCS 201, Lecture Notes in Computer Science 10703: 170-189 (2018).

16. **S. Ghilezan**, S. Jakġiĺ, J. Pantoviĺ, J. A. Pérez and H. Torres Vieira: Dynamic Role Authorisation in Multiparty Conversations, Formal Aspects of Computing 28 (4): 643ï 667 (2016).

17. Y. Gurevich, E. Hudis, J. M. Wing: Inverse Privacy, Communication of the ACM: 59 (7): 38-42 (2016).

18. J. Halpern, *Reasoning About Uncertainty*, MIT Press, 2017.

19. J. Halpern, R. van der Meyden and M. Vardi. *Complete axiomatizations for reasoning about knowledge and time*. SIAM Journal on Computing, 33, 674ï 703, 2004.

20. P. Hansen, N. Mladenoviĺ, R. Todosijeviĺ, S. Hanafi, Variable neighborhood search: basics and variants. EURO Journal on Computational Optimization 5(3), 423-454 (2017)

21. A.K. Jain, M.N. Murty, P.J. Flynn, Data clustering: a review. ACM Comput. Surv. 31(3), 264ï323 (1999). https://doi.org/10.1145/331499.331504.

22. S. Jakġiĺ, J. Pantoviĺ, **S. Ghilezan**: Linked Data Privacy, Mathematical Structures in Computer Science 27(1): 33-53 (2017).

23. X. Liang, et al. "Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability." Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (2017).

24. T. Kohonen, Essentials of the self-organizing map. Neural Netw. 37, 52ï65 (2013). https://doi.org/10.1016/j.neunet.2012.09.018. Twenty-fifth Anniversary Commemorative Issue.

25. A. Kosba et al. : Hawk -The blockchain model of cryptography and privacy-preserving smart contracts. 2016 IEEE symposium on security and privacy (SP) (2016).

26. D. Kouzapas, A. Philippou: A methodology for a formal approach in privacy, (2018).

27. B. Marinkoviĺ, P. Glavan, **Z. Ognjanović**, T. Studer, A Temporal Epistemic Logic with a Non-rigid Set of Agents for Analyzing the Blockchain protocol, Journal of logic and computation, 29(5), 803-830, (2019).

28. **M.J. Mihaljevic,** "A Security Enhanced Encryption Scheme and Evaluation of Its Cryptographic Security", *Entropy*, vol. 21 (7), July 2019 (11 pages)

29. **M.J. Mihaljevic** and F. Oggier, "Security Evaluation and Design Elements for a Class of Randomized Encryptions", *IET Information Security*, vol. 13, no. 1, pp. 36-47, Jan. 2019,

30. N. Mladenoviĺ, P. Hansen, Variable neighborhood search, Computers and Operations Research, 24(11), 1097-1100, (1997).

31. S. Nakamoto: Bitcoin: A peer-to-peer electronic cash system, Pseudonymous posting (2008). Archived at https://bitcoin.org/en/bitcoin-paper.

32. H. Nissenbaum: Privacy in Context, Stanford University Press (2010).

33. M. Ober, S. Katzenbeisser, K. Hamacher, Structure and anonymity of the Bitcoin transaction graph. Future Internet 5(2), 237ï250 (2013). https://doi.org/10.3390/fi5020237, http://www.mdpi.com/1999-5903/5/2/237.

34. **Z. Ognjanović**, M. Raġkoviĺ, Z. Markoviĺ, Probability Logics: Probability-Based Formalization of Uncertain Reasoning, Springer, 2016.

35. S. Pongnumkul, C. Siripanpornchana, S. Thajchayapong, Performance analysis of private blockchain platforms in varying workloads, in Proceedings of the 26th International Conference on Computer Communication and Networks (ICCCN) (2017), pp. 1ï6. https://doi.org/10.1109/ICCCN.2017.8038517.

36. K. Salah, M. Habib Ur Rehman, N. Nizamuddin, and A. Al-Fuqaha, ñBlockchain for AI: Review and Open Research Challengesò, *IEEE Access*, 2019.

37. D. J. Solove: A taxonomy of privacy. University of Pennsylvania Law Review, 154(3):477ï560 (2006).

38. T. Stojanoviĺ, **T. Davidović**, **Z. Ognjanović**, Bee Colony Optimization for the Satisfiability Problem in Probabilistic Logic, *Applied Soft Computing*, 31, pp. 339-347, 2015.

39. W. A. Syafruddin, S. Dadkhah and M. Köppen, "Blockchain Scheme Based on Evolutionary Proof of Work," *2019 IEEE Congress on Evolutionary Computation (CEC)*, Wellington, New Zealand, 2019, pp. 771-776.
doi: 10.1109/CEC.2019.8790128

40. D. Taylor, An Analysis of Bitcoin and the Proof-of-Work Protocols Energy Consumption Growth, Impact and Sustainability, Master thesis, Department of Mechanical and Aerospace Engineering, University of Strathclyde, Glasgow, 2018.

41. O. Tene: Privacy: The new generations. International Data Privacy Law 1(1), 15ï27 (2011).

42. D. Teodoroviĺ and M. Dell'Orco. Bee colony optimization - a cooperative learning approach to complex transportation problems. In Advanced OR and AI Methods in Transportation. Proceedings of the 10th Meeting of the EURO Working Group on Transportation, pages 51-60, Poznan, Poland, 2005.

43. S. Tomovic, **M. Mihaljevic**, A. Perovic, **Z. Ognjanovic**, A Protocol for Provably Secure Authentication of a Tiny Entity to a High Performance Computing One, Mathematical Problems in Engineering, vol. 2016, Article ID 9289050, 2016.

44. M.C. Tschantz, J.M. Wing: Formal methods for privacy. International Symposium on Formal Methods: 1-15 (2009).

45. S. D. Warren and L. D. Brandeis: The Right for Privacy, Harvard Law Review, 4, 193-220, (1890).

46. A. Westin: Privacy and Freedom. New York: Atheneum (1967).

47. X. Yue et al. "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control." Journal of medical systems 40.10 (2016): 218.

48. D. Zhang, S. Chen, Z.H. Zhou, Entropy-inspired competitive clustering algorithms. Int. J. Softw. Inform. 1(1), 67ï 84 (2007)

49. Z. Zheng et al. "An overview of blockchain technology: Architecture, consensus, and future trends." Big Data (BigData Congress), 2017 IEEE International Congress on. IEEE, 2017.

50. G. Zyskind, O. Nathan and A. Pentland: Decentralizing Privacy: Using Blockchain to Protect Personal Data. IEEE Security and Privacy Workshops, pp. 180-184 (2015).

1.2.1. Data usage

- *What types of data will the Project generate/collect?*
  The project will generate data in certain BC ledgers, and also will use data from certain already existing public BC ledgers.

- *What significant datasets are needed for the Project implementation? Specify data types and data size. Specify primary or secondary use of data.*
  The data will be used for evaluating the security and privacy issues. The data size will be determined during the project implementation and this is not a restrictive issue.

- *Do you already have access to this data, or will the data be obtained during Project implementation? If the data is to be obtained during Project implementation, specify so.*
  Certain data could be collected from already existing BC ledgers, and additional data will be generated during the project implementation.

- *How will the data be stored and accessed? What measures will be taken to ensure secure data storage and use, including data security?*
  This issue appears as not relevant because the data employed from the public BC ledgers are already public, and the data to be generated will also be considered as the public ones.

- *Who will have access to the data during Project implementation?*
  Any project member could have access to the data.

- *How will the data be used with reference to AI?*
  The data will be inputs to AI algorithms.

- *How will the costs for data curation and preservation be covered?*
  Basically ñno costsò.

- *How will these data be exploited and/or shared/made accessible for verification and re-use during and after Project implementation? If data cannot be made available, explain why.*
  Simply ï data are public.

- *Who will have access to the data after Project implementation?*
  As already claimed ï the data employed are public.

- *Who will have access to the code, or software after Project implementation ends?*
  To be decided and according suggestions after the project acceptance ï depending on the intellectual property protection approach.

1.3. Ambition

- *Describe the advance your proposal would provide beyond the state-of-the-art, and the extent to which the proposed work is ambitious.*
  Security evaluation of the BC consensus protocols and privacy issues related to the BC ledgers are already recognized and considered as important topics. This project addresses these issues from a different prospective employing AI which is an approach that has not been widely explored up to now. In the scientific literature the mentioned issues are seldom explored. The proposed approach is new, provides promising tools, and opens a bunch of new research topics.

- *Describe the novelty (e.g., ground-breaking objectives, novel concepts and approaches, new products, etc.) which the proposal represents.*
  Certain recently developed techniques of AI, non-classical logic for analysis of some BC protocols and metaheuristics for clustering in BC systems appear as novel background approaches for security evaluation of BC consensus protocols and consideration of privacy issues within BC ledgers.

- *Describe the significance of the proposed research, innovation and application potentials, and potentials for future extensions.*
  BC technology is on a sharply rising track as well as applications of AI regarding BC technology. AI and BC are proved to be quite a powerful combination, improving virtually every industry in which theyôre implemented, from food supply chain logistics and healthcare record sharing to media royalties and financial security. Therefore, the significance of the proposed research is that it provides an additional background for further advances in the addressed areas.

2. Impact

2.1. Expected impact

- *Describe the expected impact of the Project on the scientific community, society, economy, industry, healthcare, education, environment, dual use issues etc., as applicable.*
  BC technology has been recently well recognized as an important one not only from scientific point of view (because it has opened a large number of interesting research topics) but also as a technology useful for addressing a large number of society, economy, industry, healthcare, education, and environment issues. Beside other requirements, BC should provide security and privacy protection. The scientific impact of this project is straightforward because its main objectives include developing of advanced techniques based on AI for security evaluation of the BC consensus protocols and privacy protection evaluation at the BC ledger. The obtained results will hopefully be published in prestigious international journals and conferences and became accessible to the wider scientific community. High level of public interest in results of the project will be created by dissemination activities, especially by organizing an AI4TrustBC-Open Day for the representatives of IT companies, government bodies, and other potential users. This event could serve to initiate collaboration directed to solving practical problems.

- *Specify any target group or final beneficiaries who will be impacted by the Project, where applicable. Describe the type and level of impact.*
  Final beneficiaries of the project realization are within the following: the scientific community, society, economy, industry, healthcare, education, environment in the way explained above.

- *Does the Project affect any particular category of the target groups and final beneficiaries directly or indirectly, intendedly or unintendedly?*
  No.

- *Describe the mid-term and long-term impact of the Project, including the information on impact which will appear after the Project implementation.*
  The project impacts will follow the future wide spreading of BC technology and the related applications in both, the mid-term and the long-term sense. The Internet of Things (IoT), artificial intelligence (AI), and BC represent an unprecedented opportunity for the enterprise and the public sector. Every institution capable of exploiting these technologies will have a chance to radically streamline and enhance existing processes, create entirely new business models, and develop innovative products and services for a new generation of consumers. But this isnôt a vision of a utopian, tech-enabled futureð the technology capabilities are available today to help us build the business of tomorrow. The project addresses open

problems arising from rapid technological growth and develops new AI techniques of knowledge representation and privacy management based on trustworthy BC Technology. The impact is ranging from foundational to highly practical and from individual privacy protection to the society as a whole, where privacy is one of the key issues.

2.2. Dissemination of results

Dissemination strategy:

- To communicate the results at national level.
- To disseminate the results at international level.
- To reach out to the industrial, private and public sector.
- Open access.
- Web page.
- Social networks and media.

Dissemination and communication activities.

- Seminars and colloquia at MISANU are organized on a regular basis (weekly, be-monthly, monthly). Video transmission is providing availability nationally and internationally in academia and non-academic sector. This will be the basic regular dissemination tool for the entire duration of the project. http://www.mi.sanu.ac.rs/novi_sajt/research/seminars_and_colloquiums.php
- The results will be
  - communicated at some of the following international conferences:
    - International Conference on Blockchain for Science, Research and Knowledge Creation (ICBSRKC) - Boston, United State, Apr. 2021;
    - International Conference on Blockchain for Internet of Things (ICBIOT) - Jerusalem, Israel, Apr. 2021;
    - International Conference on Internet of Things and Blockchain (ICIOTB) - Tokyo, Japan, June 2021;
    - Logic and Applications 2020, 2021 Dubrovnik, Croatia;
    - ECSQARU - European Conferences on Symbolic and Quantitative Approaches to Reasoning with Uncertainty 2021;
    - JELIA - European Conference on Logics in Artificial Intelligence 2022;
    - SYMOPIS - Symposium on Operations Research 2021, 2022;
    - MOTOR - Mathematical Optimization Theory and Operations Research 2022.
  - published in international peer-reviewed scientific journals;
  - communicated to international projects in which the AI4TrustBC team is involved (H2020, COST, ERASMUS, bilateral);
  - promoted to international partners and partner institutions (Japan, China, India, USA, EU).
- The conference: ñSecurity, privacy and BC Technology for Trustful Cyberspaceò, will be organized Oct. 2020 at the Serbian Academy of Sciences and Arts, Belgrade.
- AI4TrustBC-Open Days will be organized in Belgrade and Novi Sad to present the current achievements, findings, their impact and to define practical problems and needs of the potential users of the project results. These events will follow very positive experiences gathered at the meeting "Privacy in Digital Age: Illusion or a National Challenge" (http://www.mi.sanu.ac.rs/novi_sajt/research/conferences/FPDD/index.php) organized on October 10, 2017 in the Serbian Academy of Sciences and Arts. The goal of the events is to increase the impact of project results to society and industry and establish better ties and cross-domain coordination with IT companies, government bodies, financial sector, healthcare, industry, and other potential users with an aim to initiate joint activities directed at solving their practical problems and needs, and exploiting the full potential of the scientific results. By organizing two events we hope to cover wide range of stakeholders, including MISANU's partners and particularly numerous startup companies connected to FTN.
- Research results are going to be in open access on the open science portals of MISANU, Open UNS (https://www.open.uns.ac.rs) and NAPON (Nacionalni portal otvorene nauke, http://www.open.ac.rs). Patents and tools are going to be protected and managed under intellectual property regulations.
- Creating and developing a freely accessible website of the project with access to relevant outcomes of the project, not only to the members of the project, but to all interested parties.
- Social networks and media (LinkedIn, Facebook, Twitter, Instagram) will be a regularly used to disseminate and promote the project results on a large scale.

3. Implementation Plan

3.1. Credentials of PI and the members of Project team

The research team has been chosen in such a way that it fully covers all of the necessary expertise for the delivery of the project objectives. Senior members of the team (T. Davidoviĺ, S. Ghilezan, M. Mihaljeviĺ, Z. Ognjanoviĺ and D. Uroġeviĺ) are internationally recognized experts in their research fields (see Part B of the project proposal). PhD students are recruited in the team to obtain experience in these attractive research topics.

The complementarities of the senior team members are related to the differences between their expertises:

Team member	Expertises	Objectives
T. Davidoviĺ	mathematical optimization, population based heuristic methods	to develop new Proof-of-Work tasks based on hard optimization problems and examine their performance
S. Ghilezan	formal methods and privacy	to develop knowledge reasoning techniques and formal methods for privacy management based on trustworthy BC technology
M. Mihaljeviĺ	cyber-security	to employ AI techniques to evaluate security and privacy in certain BC
Z. Ognjanoviĺ	non-classical logics, uncertain reasoning	To develop formal logic based knowledge reasoning techniques for analyzing the BC protocol
D. Uroġeviĺ	mathematical modeling, exact and heuristic solvers	to develop metaheuristic-based tools for the analysis of system security

Despite the mentioned complementarities, the strong synergy of the team members has already been established as they have already published joint scientific results (e.g., Ghilezan et al, 2018; Stojanovic et al, 2015; Tomovic et al, 2016).

Table 3.1. Members of the Project team

ID	Name and family name	Scientific and Research Organization	Person-months	Effective person-months
PI	Tatjana Davidoviĺ	Mathematical Institute SASA	24	7.2
P1	Silvia Ghilezan	Faculty of technical Sciences, University of Novi Sad	24	3.6
P2	Miodrag Mihaljeviĺ	Mathematical Institute SASA	24	7.2
P3	Zoran Ognjanoviĺ	Mathematical Institute SASA	24	7.2
P4	Dragan Uroġeviĺ	Mathematical Institute SASA	24	1.8
P5	Angelina Iliĺ -Stepiĺ	Mathematical Institute SASA	24	7.2
P6	Ġejla Dautoviĺ	Mathematical Institute SASA	24	7.2
P7	Milan Todoroviĺ	Mathematical Institute SASA	24	7.2
P8	Tamara Stefanoviĺ	Faculty of technical Sciences, University of Novi Sad	24	7.2
P9	Luka Matijeviĺ	Mathematical Institute SASA	24	3.6
P10	ņ orĽe Jovanoviĺ	Mathematical Institute SASA	24	3.6
			Total Person-months:264	Total Effective person-months:63

To fulfil the project objectives, the team members will be divided into groups as follows: S. Ghilezan and T. Stefanoviĺ (WP1); Z. Ognjanoviĺ, A. Iliĺ-Stepiĺ, and Ġ. Dautoviĺ (WP1); T. Davidoviĺ, D. Uroġeviĺ, L. Matijeviĺ, and ṇ. Jovanoviĺ (WP2) to develop the proposed knowledge reasoning methodologies. M. Mihaljeviĺ and M. Todoroviĺ will perform preparatory work in WP3. M. Mihaljeviĺ will be involved in WP1 and WP2 to support the development of the proposed techniques and to guarantee their applicability to BC. In the second phase of the project, these groups will collaborate to employ the developed methodologies in the analysis of certain BCs (WP3). The partner SROs will provide the adequate research infrastructure (space, libraries, Internet, access to WoS and SCOPUS services). In addition, partner SROs will support the organization of AI4TrustBC-Open Days in Belgrade and Novi Sad.

3.2. Implementation plan

The Project **implementation plan** involves 4 work packages (WP). Within WP1 formal knowledge reasoning techniques and methods for privacy management and analysis of consensus algorithms for BC will be developed. WP2 will be devoted to the development of metaheuristics based methods for design and performance evaluation of consensus protocols and evaluation of privacy protection robustness for BC. After the preparatory activities in WP3 (reviewing the consensus protocols and ledgers generated within certain BC and selecting the ones to be subject of the security evaluation by the developed methodologies), outputs of WP1 and WP2 will be applied to the selected BCs. The project management activities (coordination with other WP leaders, budget maintenance, dissemination) will be performed in WP4.

Table 3.2a: List of work packages (WP)

WP No	WP title	WP Lead SROôs acronym	WP Lead - team memberôs ID	Start month	End month	Total calendar months of WP duration
1	Developing knowledge reasoning techniques and formal methods	FTN	P1	1	24	24
2	Developing metaheuristic-based tools for BC	MISANU	P4	1	24	24
3	Security/Privacy Evaluation of BC Consensus/Ledger	MISANU	P2	1	24	24
4	Management	MISANU	PI	1	24	24

Table 3.2b: Work package description

Work package number	1	Work package title	Developing knowledge reasoning techniques and formal methods
Lead SROôs acronym	FTN, MISANU		
Team member ID	P1, P2, P3, P5, P6, P8		

Objectives
O1.1 to develop formal logic based Knowledge reasoning techniques for analyzing the BC protocol
O1.2 to develop knowledge reasoning techniques and formal methods for privacy management based on trustworthy BC technology

Description of work (where appropriate, broken down into sub-activities), and role of team members

WP1 will investigate and develop formal knowledge reasoning techniques and methods for privacy management based the BC protocol and analysis of consensus algorithms for the BC protocol.

The tasks of this work package will be as follows:

T1.1 Introducing a probabilistic temporal epistemic logic (to define a formal language, syntax and semantics, and to give an axiom system).
T1.2 Analyzing the logic and prove the main theorems about the logic (soundness, strong completeness, decidability).
T1.3 Describing the BC protocol using the proposed logic and analyzing properties of the BC protocol, particularly its consensus algorithms.
T1.4. Developing robust extensions of concurrent and process models for formalization of decentralized privacy in BC technology and proving liveness, correctness and safety.
T1.5. Exploring new concepts of privacy based on known concepts of differential, contextual and inverse privacy in order to handle privacy issues suitable for trustworthy BC technology.
T1.6. Developing a tool for privacy management based on trustworthy BC technology.
T1.7. Performing a comparative analysis of existing tools for privacy management.

Links with other WPs: WP1 works with WP3 to apply developed formal methods and techniques to analyze the BC protocol.

Role of team members: P1 will coordinate the investigation carried out in this WP. P3, P5 and P6 will be responsible for T1.1-T1.3. P1 and P8 will be responsible for T1.4-T1.7. P2 will be involved in T1.3 and T1.7 to ensure that the developed formal methods and techniques are suitable to analyze the BC protocol.

Deliverables of the work package (brief description and month of delivery)

D1.1 (Month 7) A report defining the formal probabilistic temporal epistemic logic
D1.2 (Month 10) A report on a strongly complete axiomatization of the logic
D1.3 (Month 12) A report on analyzing decidability of the logic
D1.4 (Month 18) A report giving a formal description of the BC protocol
D1.5 (Month 7) A report describing models for privacy management
D1.6 (Month 9) A report giving a comparative analysis of differential privacy, contextual privacy and inverse privacy
D1.7 (Month 12) An environment for privacy management based on trustworthy BC technology
D1.8 (Month 18) A report on the comparative analysis of existing tools for privacy management

Work package number	2	Work package title	Developing metaheuristic-based tools for BC
Lead SROôs acronym	MISANU		
Team member ID	PI, P4, P9, P10 & P2		

Objectives:
O2.1: to develop new Proof-of-Work tasks based on hard optimization problems and examine their performance;
O2.2: to develop metaheuristic-based tools for the analysis of system security.

Description of work (where appropriate, broken down into sub-activities), and role of team members

Within WP2 we will explore the metaheuristics to design and performance evaluation of consensus protocols and to evaluate robustness of the privacy protection in BC technology.
The following sub-activities (tasks) can be identified:
T2.1: Studying literature and identifying potential points of interests in both related topics (PI, P4, P9, P10).
T2.2: Selection and instalation of proper BC platforms and implementations for further analysis (PI, P4, P9, P10).
T2.3: Developing of metaheuristic-based consensus protocols and their evaluation (PI, P9, P10)
T2.4: Developing of metaheuristic-based clustering and post-clustering analysis and their evaluation (P4, P9, P10)
T2.5: Preliminary evaluation (PI, P2, P4, P9, P10)

Links with other WPs: WP2 works with WP3 to apply developed tools and examine their performance with respect to the existing approaches.

Role of team members: P4 will coordinate activities within WP2 and participate in the implementation tasks. PI, P9, P10 will implement and evaluate the proposed metaheuristic-based tools. P2 will ensure that the developed formal methods and techniques are suitable to analyze the BC protocol.

Deliverables of the work package (brief description and month of delivery)

D2.1 (Month 4) A report describing state-of-the-art tools from the relevant literature and topics for further investigation
D2.2 (Month 8) Activation of selected BC platforms and short user manual
D2.3 (Month 12) An implementation of metaheuristic-based clustering (codes and documentation)
D2.4 (Month 15) An implementation of metaheuristic-based consensus protocol (codes and documentation)
D2.5 (Month 18) A report describing application and preliminary evaluation of the proposed methodology

Work package number	3	Work package title	Security/Privacy Evaluation of BC Consensus/Ledger
Lead SROôs acronym	MISANU		
Team member ID	P2, P7-P8 & P1, P3, P5, P6, P8 & PI, P4, P9, P10		

Objectives
O3.1: Security evaluation of certain BC consensus protocols employing techniques of AI.
O3.2: Privacy evaluation of certain BC ledgers employing techniques of AI.

Description of work (where appropriate, broken down into sub-activities), and role of team members

Description
The work consists of the following two main phases: (i) the preparation analysis to be performed within the task T3.1 and T3.2; and (ii) the evaluation phase to be performed within the tasks T3.3 and T3.4.
T3.1: Review of the consensus protocols and selection of the ones to be subject of the security evaluation
T3.2: Review of the ledgers generated within certain BC applications and selection of the ones to be subject of the privacy evaluation.
T3.3: Security evaluation of the consensus protocols selected in T1 employing approaches from WP1.
T3.4: Evaluation of the privacy issues at the BC ledgers selected in T2 employing approaches from WP1 and WP2

Links with other WPs: As given above regarding T3.3 and T3.4.

Role of team members: .
P2 is coordinator of all activities within T3.1-T3.4, and the principal investigator regarding T3.1 and T3.2.
T3.1 and T3.2 will be mainly realized by P2, P7 and P8 with consulting support from PI, P1, P3 and P4.
T3.3 will be jointly realized by P2, P7 and P1, P3, P5, P6, P8.
T3.4 will be jointly realized by P2, P7 and PI, P4, P9, P10 and P1, P3, P5, P6, P8.

Deliverables of the work package (brief description and month of delivery)

D3.1. Report on the BC consensus protocols selected for the security evaluation (month 6)

D3.2. Report on the BC ledgers selected to be subject of privacy evaluation (month 8)

D3.3. Report on the security evaluation of certain BC consensus protocols (month 24)

D3.4. Report on the privacy evaluation of certain BC ledgers (month 24)

Work package number	4	Work package title	Management
Responsible SRO	MISANU		
Team member ID	PI		

Objectives:
O4.1: Coordination of project activities, maintaining schedules and correcting potential deviations.

Description of work (where appropriate, broken down into sub-activities), and role of team members

Coordination with other WP leaders, budget maintenance, dissemination of project. The aim of this WP is to provide financial, legal, and other management activities necessary in a project of this kind. Within this WP activities related to dissemination (creating the project website and FB-page, organizing two AI4TrustBC-Open Days in Belgrade and Novi Sad) will be organized by the technical departments of MISANU and FTN (expenses expressed in the MISANU and FTN overhead section of the budget).

Deliverables of the work package (brief description and month of delivery)

D4.1 (Month 3) AI4TrustBC-website and Facebook-page

D4.2 (Month 3) Quartile report about progress of the project

D4.3 (Month 6) A report about project results (to be update every 3 months)

D4.4 (Month 15) Presentation of project and the obtained results at MISANU Seminar

D4.5 (Month 18) AI4TrustBC-Open Days

D4.6 (Month 20) A report about Open Day meetings

- Present the major deliverables of the Project matching the deliverables presented for each work package.

Table 3.2c: Major Deliverables

Deliverable ID	Deliverable name	WP No	Month of delivery
D1.1	A report defining the formal probabilistic temporal epistemic logic	WP1	7
D1.2	A report on a strongly complete axiomatization of the logic	WP1	10
D1.3	A report on analyzing decidability of the logic	WP1	12
D1.4	A report giving a formal description of the BC protocol	WP1	18
D1.5	A report describing models for privacy management	WP1	7
D1.6	A report giving a comparative analysis of differential privacy, contextual privacy and inverse privacy	WP1	9
D1.7	An environment for privacy management based on trustworthy BC technology	WP1	12
D1.8	A report on the comparative analysis of existing tools for privacy management	WP1	18
D2.1	A report describing state-of-the-art tools from the relevant literature and topics for further investigation	WP2	4
D2.2	Activation of selected BC platforms and short user manual	WP2	8
D2.3	An implementation of metaheuristic-based clustering (codes and documentation)	WP2	12
D2.4	An implementation of metaheuristic-based consensus protocol (codes and documentation)	WP2	15
D2.5	A report describing application and preliminary evaluation of the proposed methodology	WP2	18
D3.1	Report on the methodology framework for knowledge reasoning techniques and algorithms for clustering and PoW	WP3	6
D3.2	Report on the BC consensus protocols and ledgers selected to be subject of security and privacy evaluation	WP3	8
D3.3	Report on the security evaluation of certain BC consensus protocols	WP3	24
D3.4	Report on the privacy evaluation of certain BC ledgers	WP3	24
D4.1	AI4TrustBC-website and Facebook-page	WP4	3
D4.2	Quartile report about progress of the project	WP4	3
D4.3	A report about project results (to be update every 3 months)	WP4	6
D4.4	Presentation of project and the obtained results at MISANU Seminar	WP4	15
D4.5	AI4TrustBC-Open Days	WP4	18
D4.6	A report about Open Day meetings	WP4	20

- Present a list of milestones which will map the progress in achieving the objectives of each work package.

Table 3.2.d: Milestones

Milestone ID[1]	Milestone name	Means of verification	WP No	Due month[2]
M1.1	Agreement on methodology framework for knowledge reasoning techniques	Agreement among WPs communicated to PI	1,3	6
M1.2	Formal probabilistic temporal epistemic logic established	A report published on the arXiv.org	1	9
M1.3	BC protocol and privacy analyzed using the knowledge reasoning techniques	A report published on the arXiv.org	1	18
M2.1	Agreement on algorithms for clustering and PoW	Agreement among WPs communicated to PI	2,3	6
M2.2	Metaheuristic-based tools for clustering in BC	Program code and documentation	2	12
M2.3	Metaheuristic-based PoW tasks implementation	Program code and documentation	2	15
M3.1	Agreement on methodology framework for knowledge reasoning techniques	Agreement among WPs communicated to PI	1,3	6
M3.2	Agreement on algorithms for clustering and PoW	Agreement among WPs communicated to PI	2,3	6
M4.1	Financing provided for the second year of the project	Annual report approved by the Program Committee of The Fund	4	14
M4.2	Feedback from Open Day participants	A report about Open Day meeting	4	20

[1] The ID should be composed as M1.1 where the first number represents the number of WP, while the second refers to the number of the particular milestone. In case you have several milestones for one WP, please mark them as M1.1, M1.2 etc.

[2] Month in Project. Data should match the Gantt Chart.

- Present the costs of all budget categories of the Project.

Table 3.2.e: Budget

Budget category[3]	**Costs in EUR**	**% of budget**
Personnel	97,168.05	55.17
Travel	0	0
Conferences and publications	26,400.00	14.99
Equipment	36,355.93	20.64
Consumables	0	0
Services and subcontracting	1,200.00	0.68
Dissemination	4,000.00	2.27
Other costs	0.00	0.00
SROs overhead	11,000.00	6.25
Total	**176,123.98**	**100**

- Provide a short narrative description of all budget categories of the Project.

3.3. Risk management

Table 3.3. Risk management

Risk assessment	Description of the risk	Risk mitigation measure to be undertaken by members of the Project team or SRO	Risk level[4]
Methodology risk	Description of the risk[5]	Methodology appears as inappropriate	low
	Actions to be undertaken	The project team includes experts in their research fields. Interaction among them will ensure that the proper changes of the methodology will be proposed	
Work packages, deliverables and milestones	Description of the risk	The objectives/deliverables/milestones cannot be achieved	low
	Actions to be undertaken	Adapt the objectives/deliverables/milestones to the closest ones which are achievable	
Members of the project team and SROs	Description of the risk	Members of the project team appear as unavailable	low
	Actions to be undertaken	Employ additional members or redistribute the jobs over the available members	
Procurement	Description of the risk	Not relevant	/
	Actions to be undertaken	/	
Budgetary issues	Description of the risk	Shortage of the budget	low
	Actions to be undertaken	Reduction of the budget spending	
Other risks	Description of the risk		
	Actions to be undertaken		

This is the end of Project Description Part A; please continue to Project Description Part B.

[3] Make sure to include any significant items of technical equipment, relevant to the Project proposal, as well as software.

[4] Indicate risk level as high/medium/low.

[5] Insert more rows according to the number of detected risks.