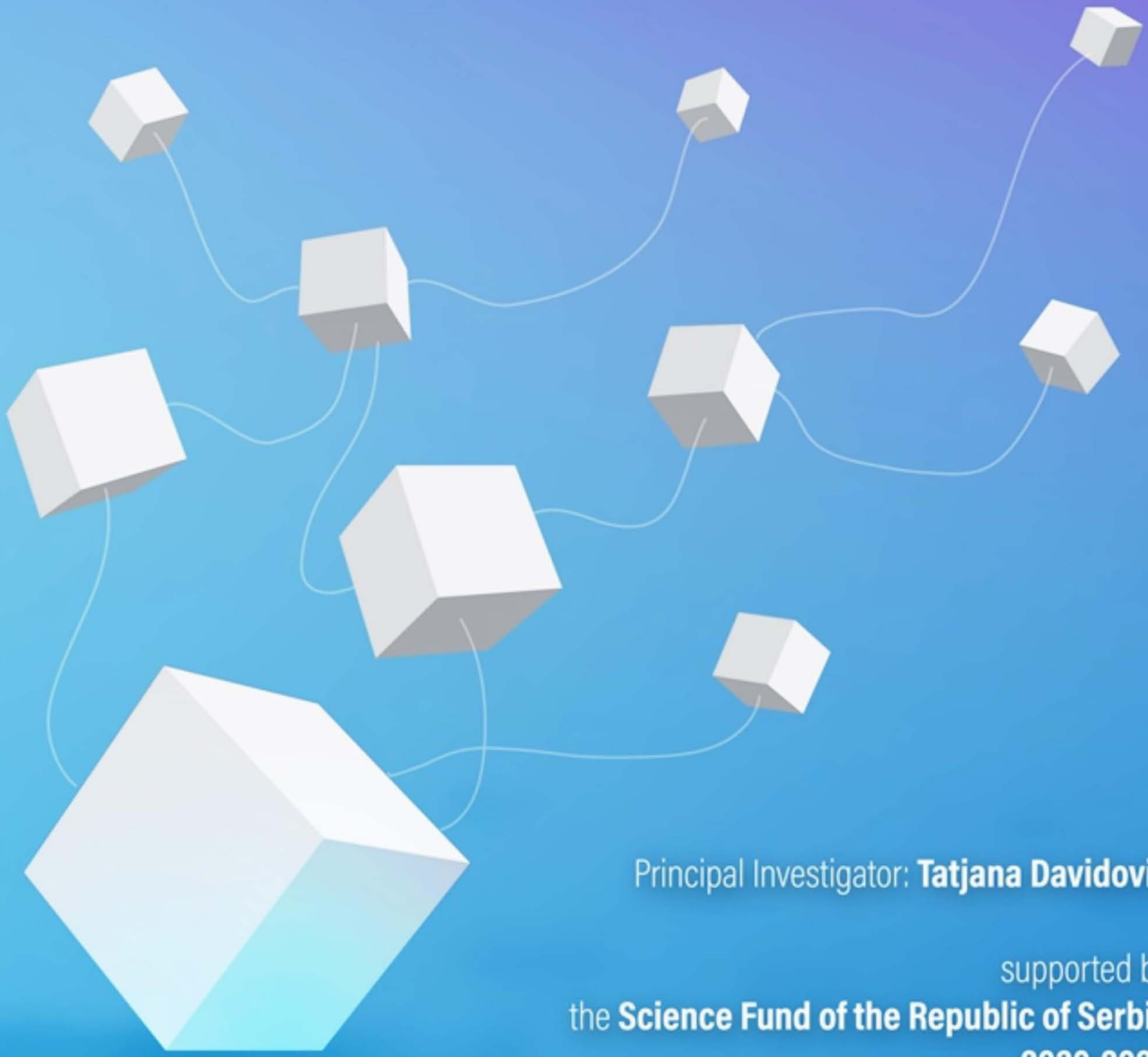
Project **AI4TrustBC**

Advanced Artificial Intelligence Techniques for Analysis and Design of System Components Based on Trustworthy BlockChain Technology



Principal Investigator: **Tatjana Davidović**

supported by
the **Science Fund of the Republic of Serbia**
2020-2022

Фонд за науку
Републике Србије

Математички институт
САНУ

Project structure - Workpackages

WP1 - Developing Knowledge Reasoning Techniques and Formal Methods for BC

Objectives:

- **O1.1.** Development of formal logic based Knowledge reasoning techniques for analyzing the BC protocol
- **O1.2.** Development of knowledge reasoning techniques and formal methods for privacy management based on trustworthy BC technology

WP1

WP2 - Developing Metaheuristic-based Tools for BC

Objectives:

- **O2.1.** Development of new Proof-of-Work tasks based on hard optimization problems and examination of their performance;
- **O2.2.** Development of metaheuristic-based tools for the analysis of system security.

WP2

WP3 - Security/Privacy Evaluation of BC Consensus/Ledger

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.

WP3

WP4 - Project Management

Objectives:

- **O4.1.** Coordination of project activities, maintaining schedules and correcting potential deviations.

WP4

Abstract:

List of Researchers:

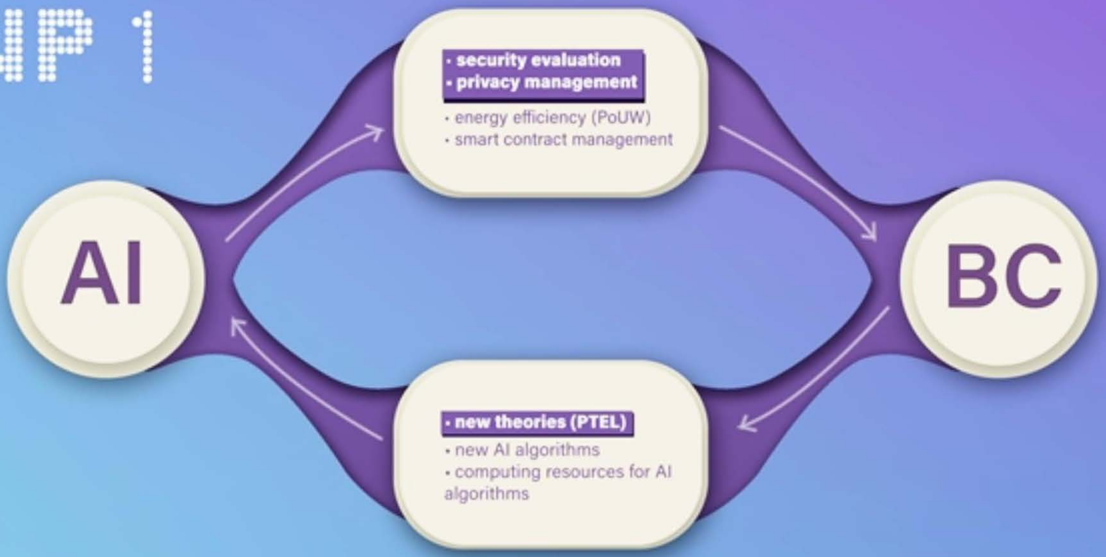
AI4TrustBC

Фонд за науку
Републике Србије

Математички институт
САНУ

Sinergy Between Artificial Intelligence and BlockChain

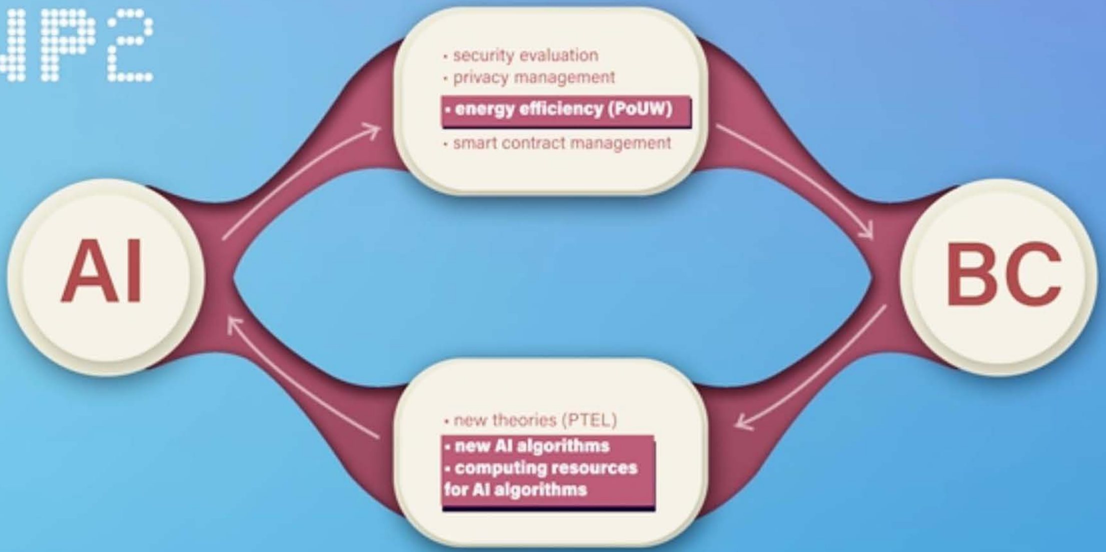
WP 1



- **security evaluation**
- **privacy management**
- energy efficiency (PoUW)
- smart contract management

- **new theories (PTEL)**
- new AI algorithms
- computing resources for AI algorithms

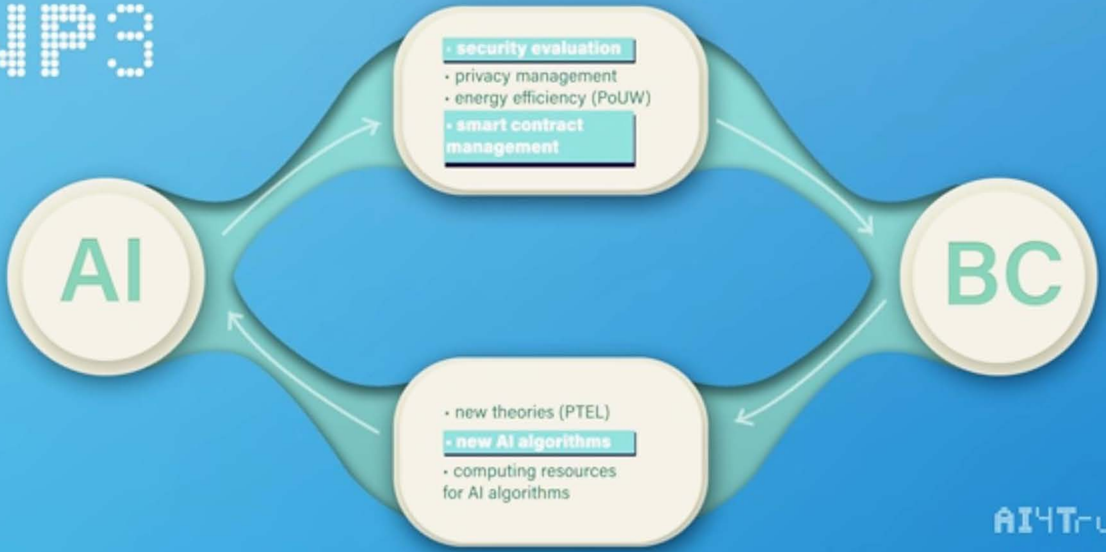
WP2



- security evaluation
- privacy management
- **energy efficiency (PoUW)**
- smart contract management

- new theories (PTEL)
- **new AI algorithms**
- **computing resources for AI algorithms**

WP3



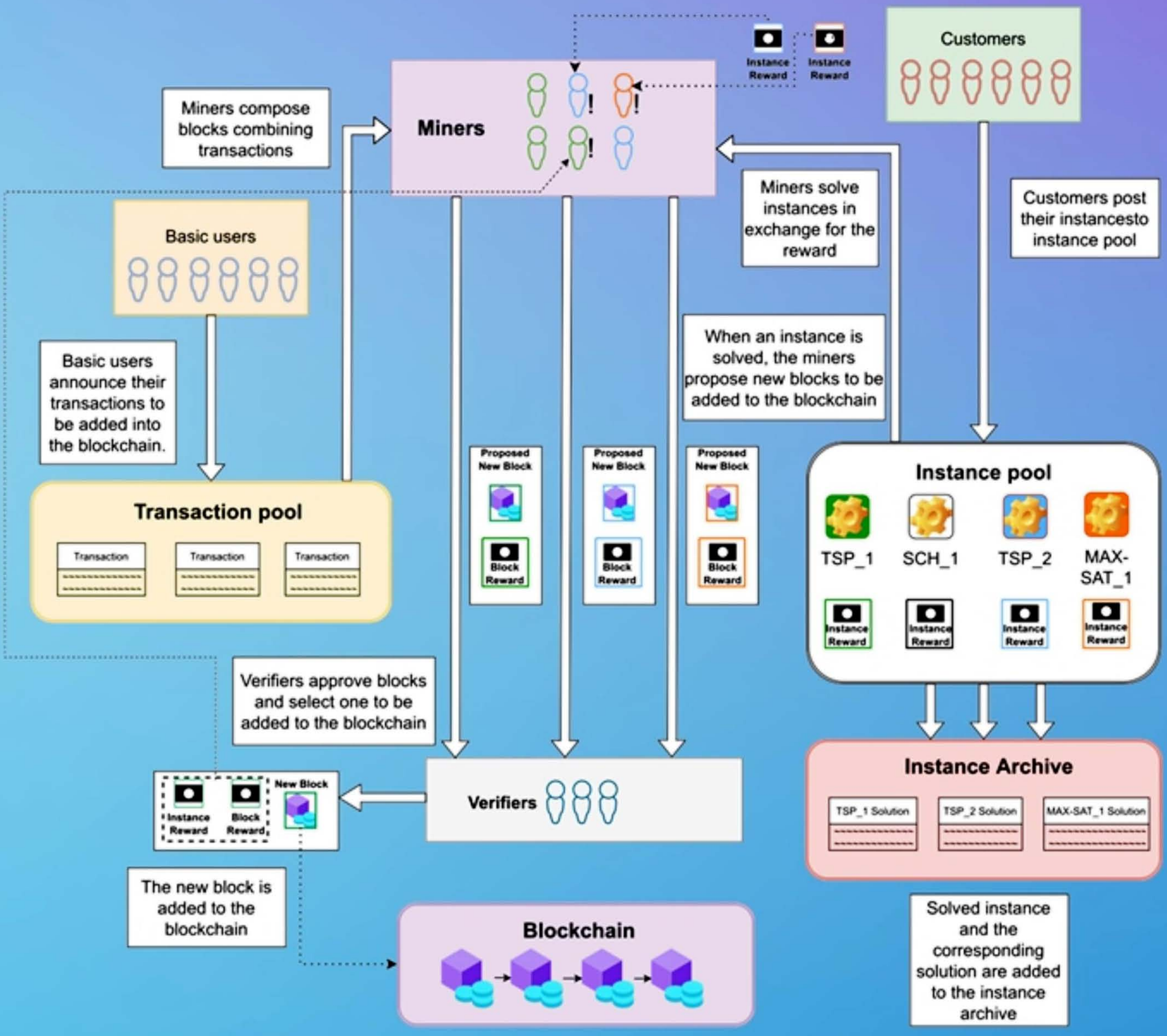
- **security evaluation**
- privacy management
- energy efficiency (PoUW)
- **smart contract management**

- new theories (PTEL)
- **new AI algorithms**
- computing resources for AI algorithms

AI4TrustBC

Фонд за науку
Републике Србије

PoUW-based Blockchain System



Customers

Customers post their instancesto instance pool

Miners

Instance Reward

Instance Reward

Miners compose blocks combining transactions

Miners solve instances in exchange for the reward

Basic users

Basic users announce their transactions to be added into the blockchain.

Transaction pool

Transaction

Transaction

Transaction

When an instance is solved, the miners propose new blocks to be added to the blockchain

Proposed New Block

Block Reward

Proposed New Block

Block Reward

Proposed New Block

Block Reward

Instance pool

TSP_1

SCH_1

TSP_2

MAX-SAT_1

Instance Reward

Instance Reward

Instance Reward

Instance Reward

Verifiers approve blocks and select one to be added to the blockchain

Verifiers

Instance Reward

Block Reward

New Block

The new block is added to the blockchain

Blockchain

Instance Archive

TSP_1 Solution

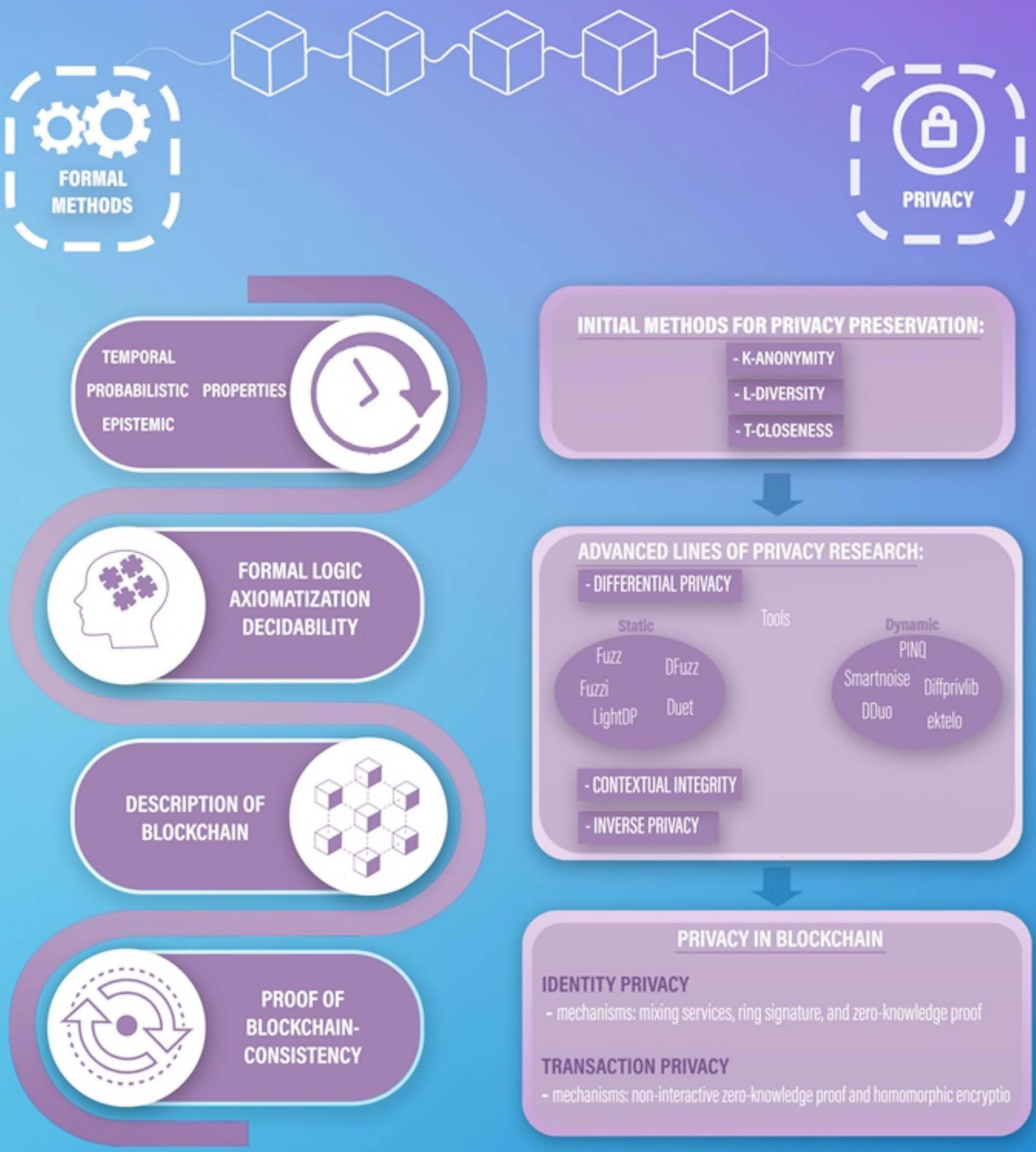
TSP_2 Solution

MAX-SAT_1 Solution

Solved instance and the corresponding solution are added to the instance archive

AI4TrustBC

BLOCKCHAIN



FORMAL METHODS

PRIVACY

TEMPORAL
PROBABILISTIC PROPERTIES
EPISTEMIC

FORMAL LOGIC
AXIOMATIZATION
DECIDABILITY

DESCRIPTION OF BLOCKCHAIN

PROOF OF BLOCKCHAIN-CONSISTENCY

INITIAL METHODS FOR PRIVACY PRESERVATION:

- K-ANONYMITY
- L-DIVERSITY
- T-CLOSENESS

ADVANCED LINES OF PRIVACY RESEARCH:

- DIFFERENTIAL PRIVACY

Tools

Static: Fuzz, DFuzz, Fuzzi, LightDP, Duet

Dynamic: PINQ, Smartnoise, Diffprivlib, DDuo, ektelo

- CONTEXTUAL INTEGRITY
- INVERSE PRIVACY

PRIVACY IN BLOCKCHAIN

IDENTITY PRIVACY

- mechanisms: mixing services, ring signature, and zero-knowledge proof

TRANSACTION PRIVACY

- mechanisms: non-interactive zero-knowledge proof and homomorphic encryptio

AI4TrustBC

Фонд за науку
Републике Србије

BubbleAntiCovid19 - *BAC19*

FEDERATING DIGITAL CONTACT TRACING USING STRUCTURED OVERLAY NETWORKS

COVID PANDEMICS

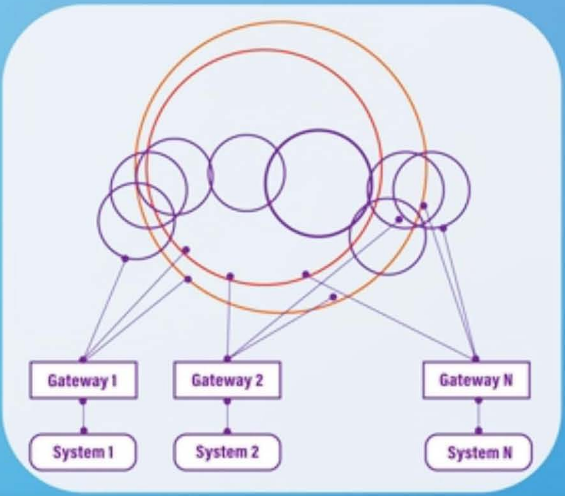
GOAL: SLOW DOWN THE SPREADING OF SARS-CoV-2 VIRUS

MEANS: CONTACT TRACING

TOOLS: DCT - DIGITAL CONTACT TRACING APPLICATIONS

PROBLEM: NO INTEROPERABILITY

SOLUTION: BubbleAntiCovid19 - *BAC19*



BAC19 ARCHITECTURE:

- CONNECTS DIFFERENT DCT APPLICATIONS

- CONSISTS OF CHORD NETWORKS CONNECTED BY SYNAPSE NODES

BAC19 ADVANTAGES:

- DOES NOT STORE ANY PERSONAL INFORMATION

- SUPPORTS MANUAL ENTRY OF CONTACTS

- NO NEW HIGHLY COMPLICATED CALCULATIONS

-SIMULATION IN PYTHON

Authors:
Silvia Ghilezan
Luigi Liquori
Bojan Marinković
Simona Kašterović
Zoran Ognjanović
Tamara Stefanović

AI4TrustBC