WP3 - Security/Privacy Issues of Blockchain Consensus/Ledger

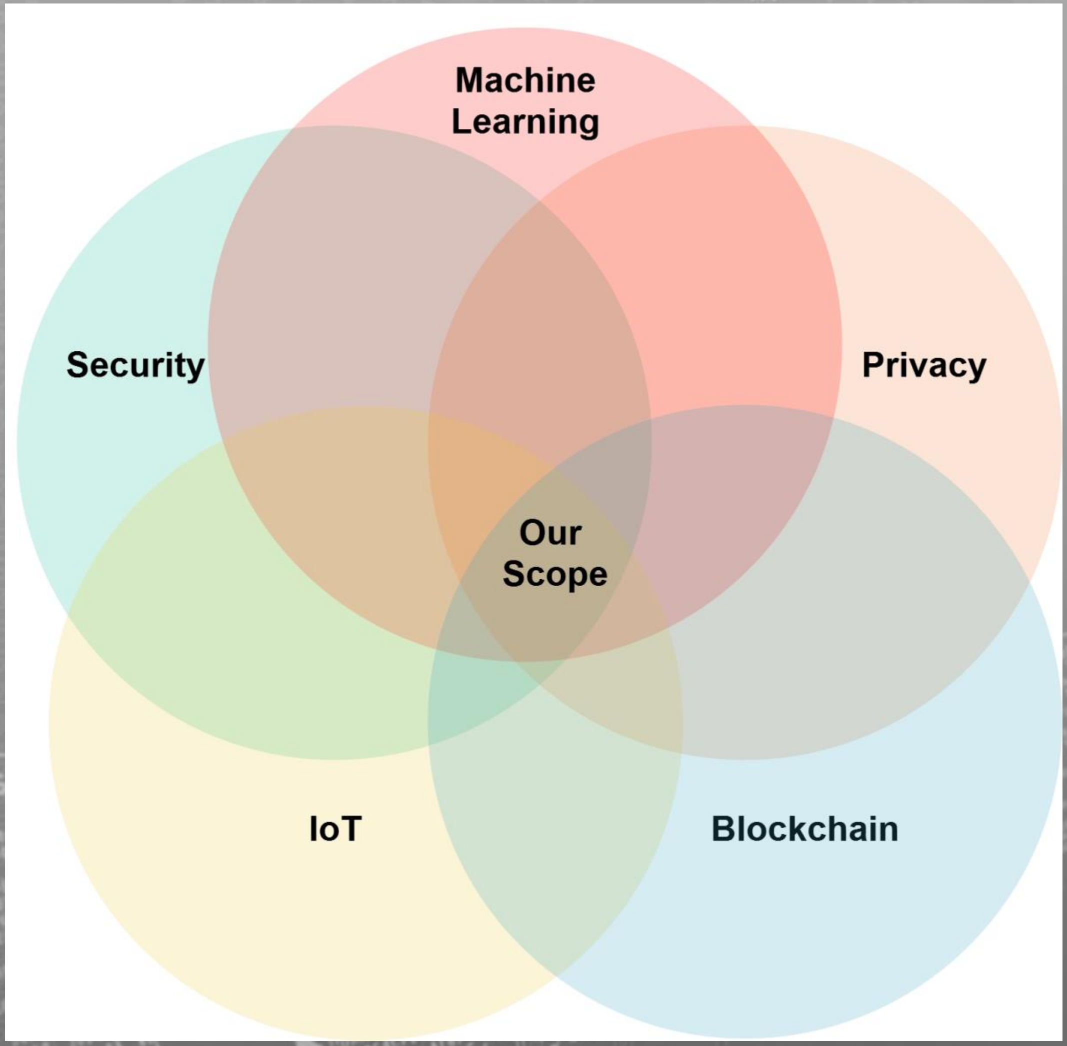
Miodrag Mihaljević

Presentation of the Project AI4TrustBC
16 May 2022

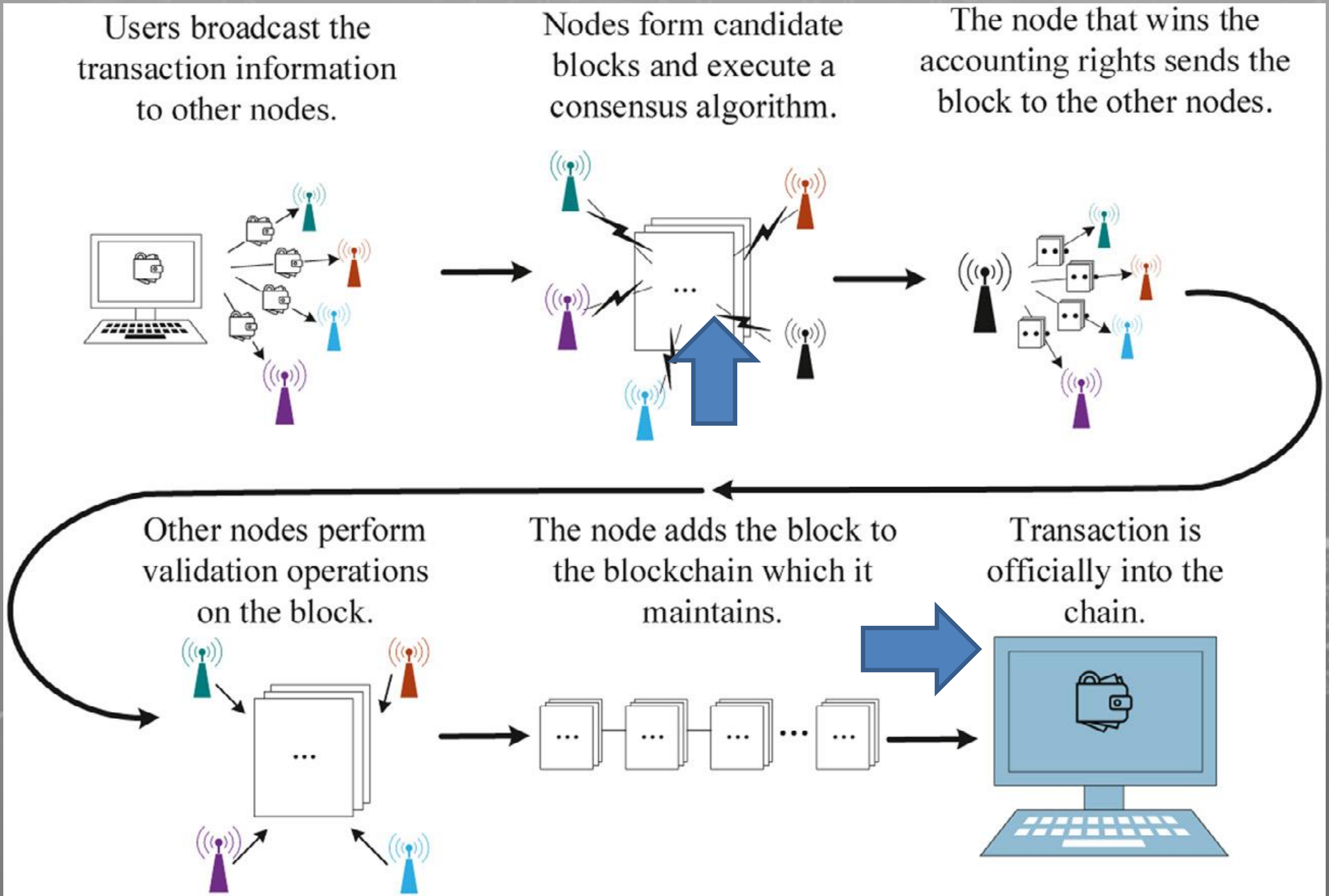
1. Objectives of WP3 AI4TrustBC

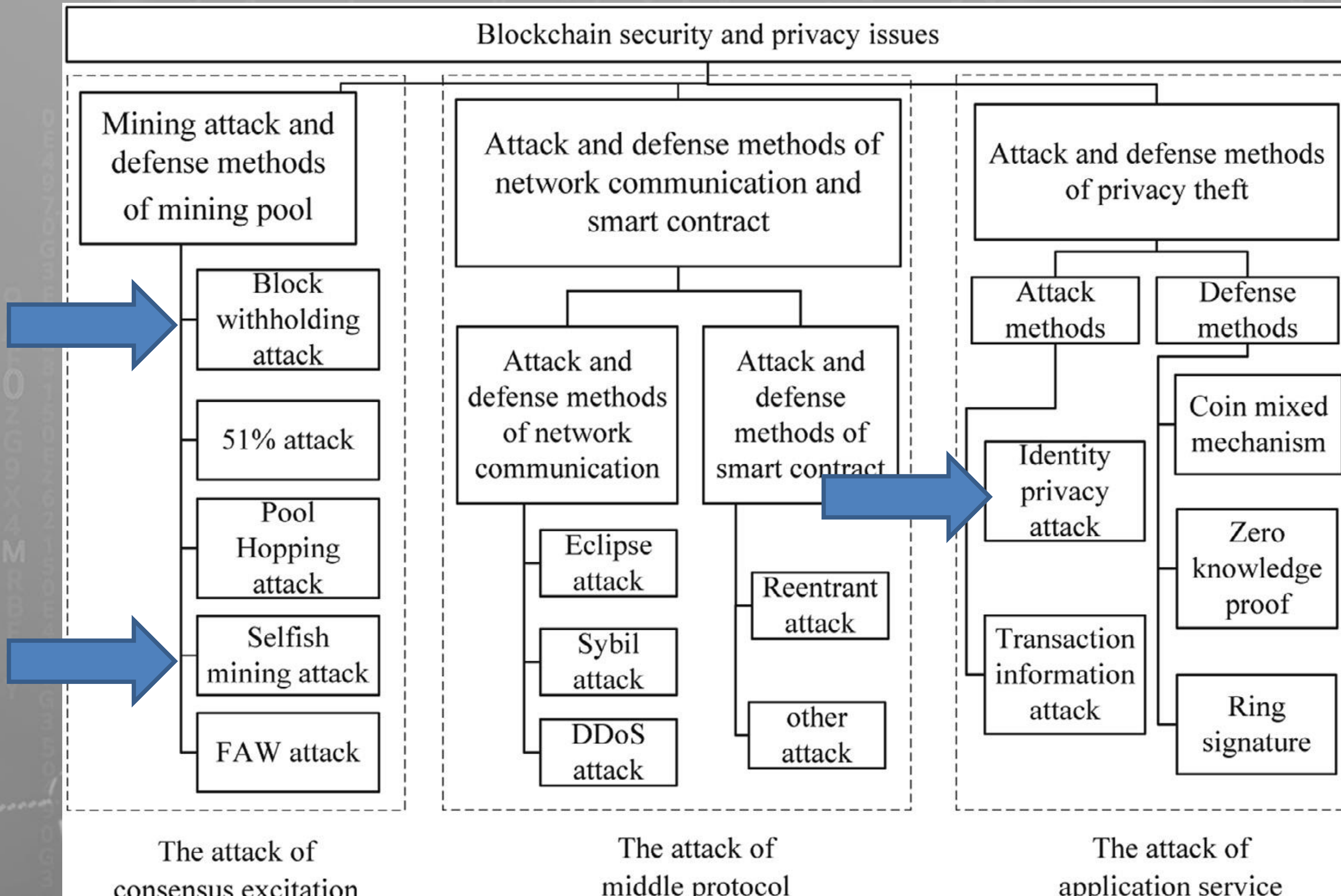
- Security evaluation of certain BC consensus protocols employing techniques of AI
- Privacy evaluation of certain BC ledgers employing techniques of AI

Illustration of WP3 Scope



Workflow of a Blockchain



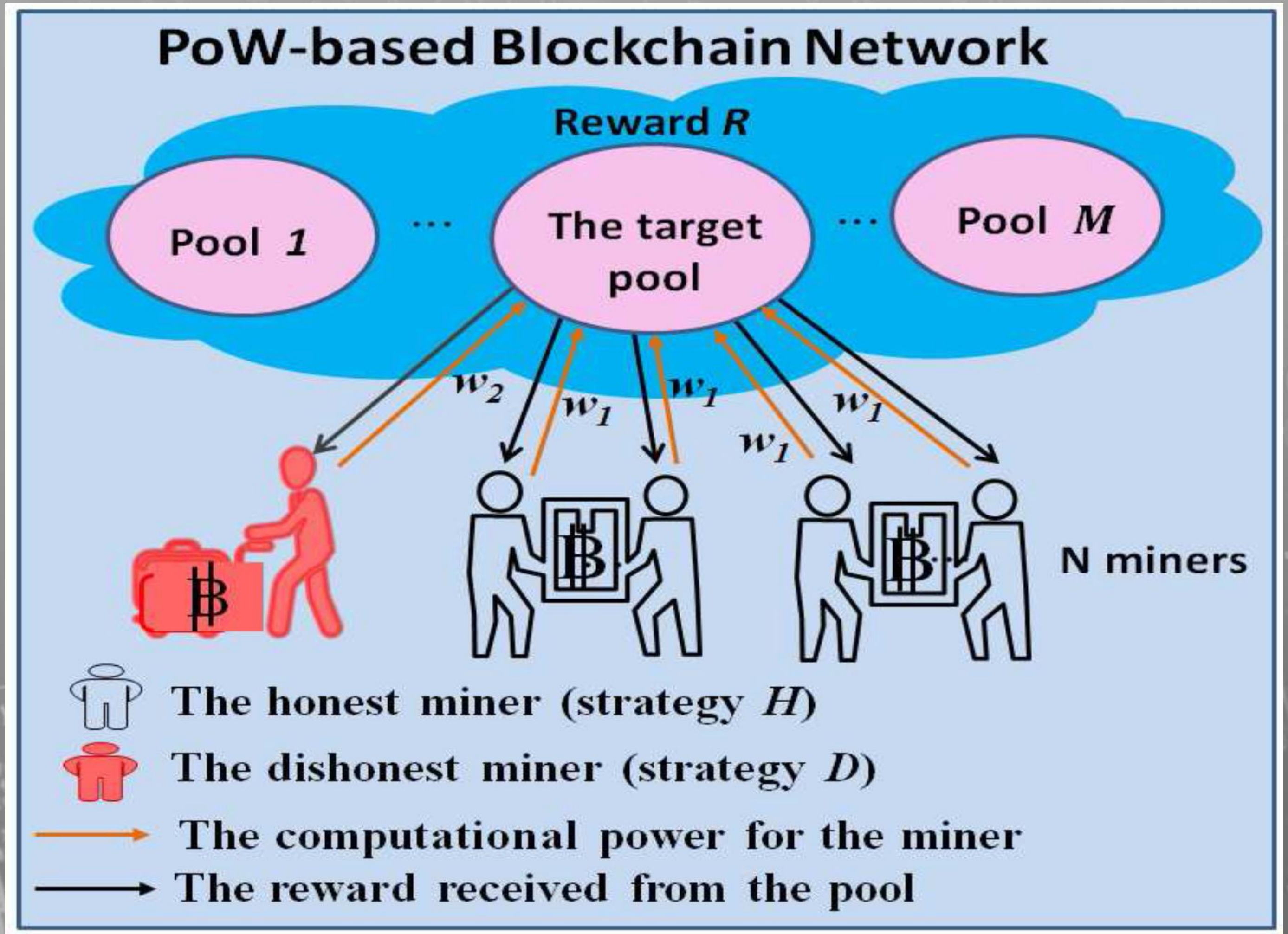

Blockchain security and privacy issues
Mining attack and defense methods of mining pool
Block withholding attack
51% attack
Pool Hopping attack
Selfish mining attack
FAW attack
Attack and defense methods of network communication and smart contract
Attack and defense methods of network communication
Eclipse attack
Sybil attack
DDoS attack
Attack and defense methods of smart contract
Reentrant attack
other attack
Attack and defense methods of privacy theft
Attack methods
Identity privacy attack
Transaction information attack
Defense methods
Coin mixed mechanism
Zero knowledge proof
Ring signature
The attack of consensus excitation
The attack of middle protocol
The attack of application service

2. SECURITY EVALUATION OF CERTAIN BC CONSENSUS PROTOCOLS EMPLOYING TECHNIQUES OF AI

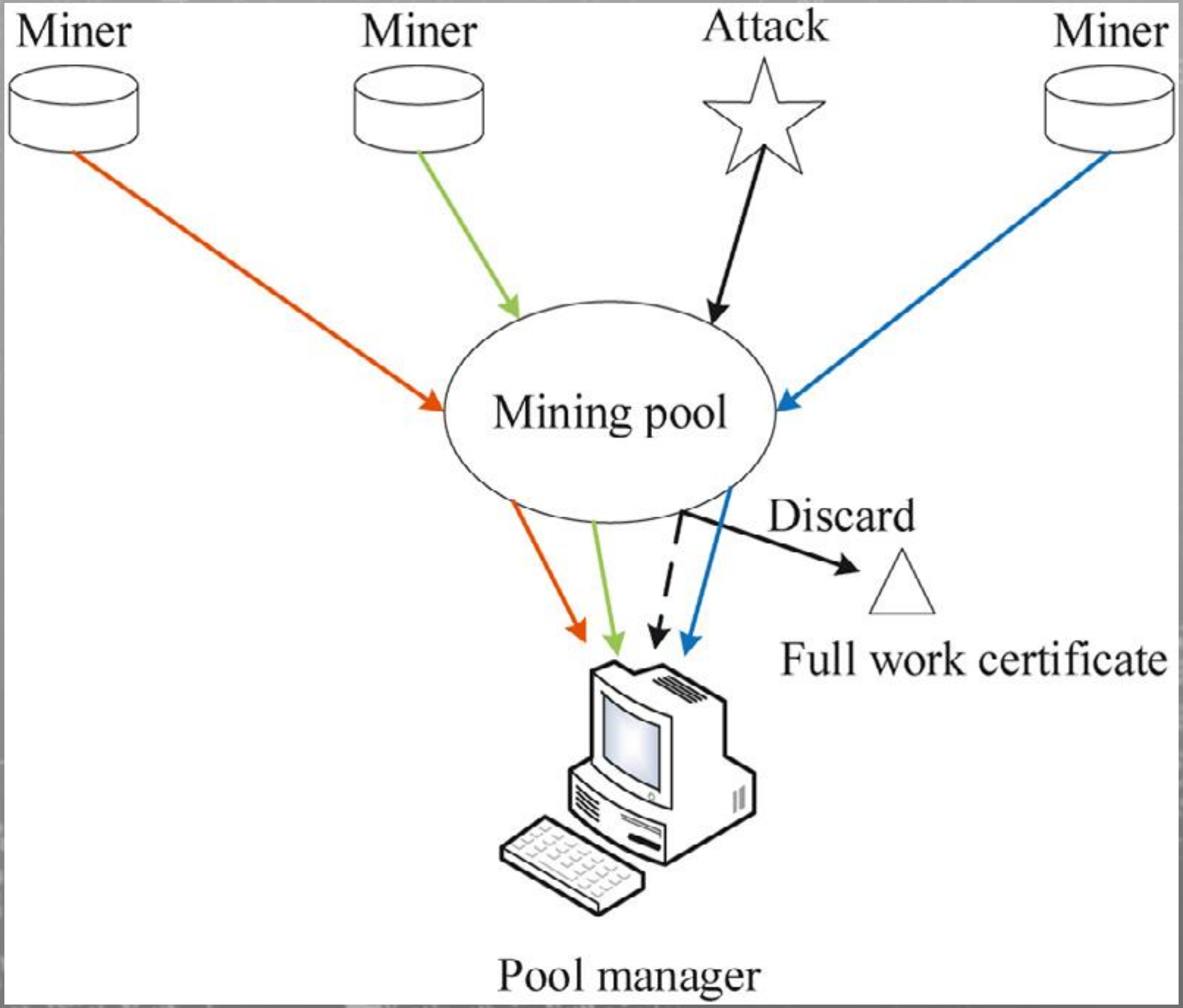
Pool Mining Paradigm

- Pool mining is the dominant approach for the participation of a miner in a blockchain system, particularly in public blockchain systems that involve proof-of-work-based consensus protocols.
- Pool mining provides a miner with a working framework that preserves the return of mining investment because a miner will be rewarded for the working efforts even if they do not yield the mining solution
- Taking into account difficulty in finding the valid solution of the cryptographic puzzle, the operator of the pool will reward participating miners based on the working efforts for solving the subpuzzles distributed to the miners.
- The difficulty of a subpuzzle is much smaller than the challenging puzzle, and the miners can find the solutions of the sub-puzzles with a reasonable effort.
- The operator of the pool will let its miners submit as many solutions of the subpuzzles as they can and distribute the rewards among its miners according to their submitted solutions.

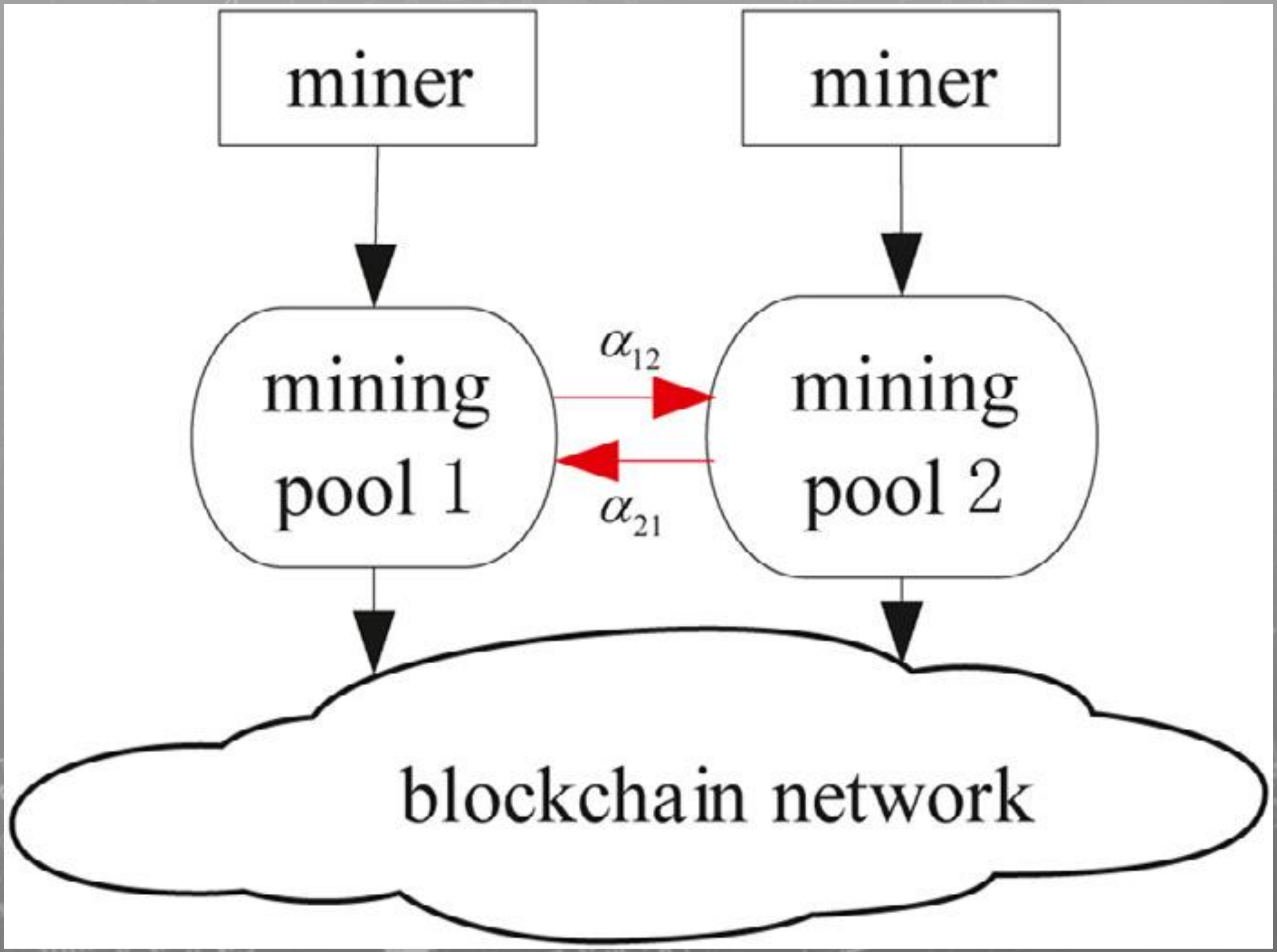
Dishonest Miners & Pool Mining within Permissionedless Blockchain



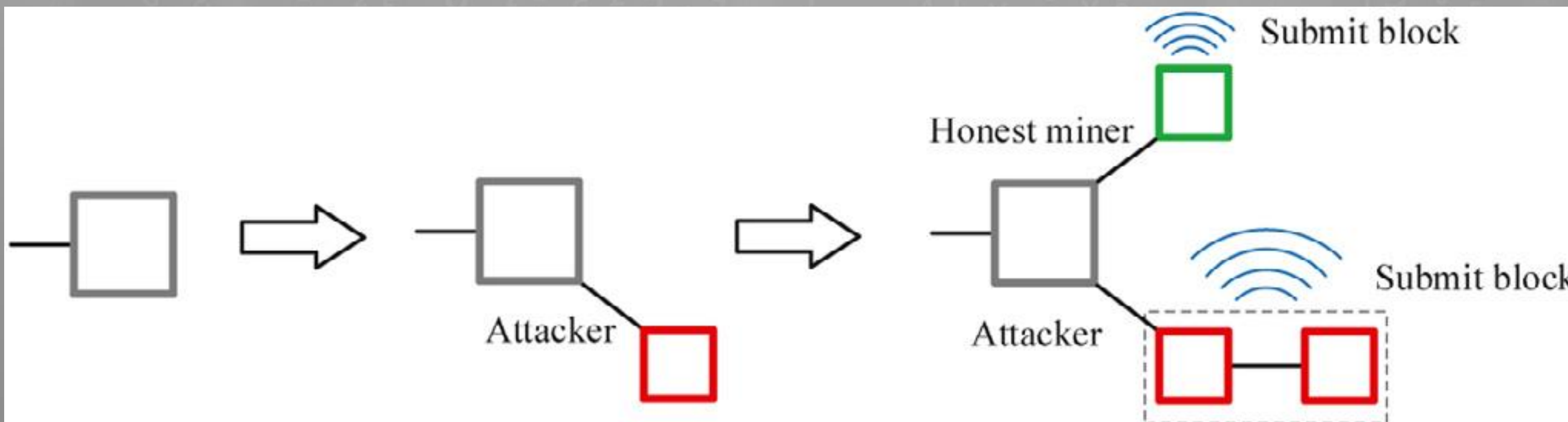
Pool Mining and Block Withholding Attack (1)



Pool Mining and Block Withholding Attack (2)



Selfish Mining



Defence Against Block Withholding and Selfish Mining Attacks

- Employment of AI techniques for detecting dishonest work of the malicious miners.
- Illustration: Game Theory and Deep Learning

- Developing blockchain approaches highly resistant against block withholding and selfish mining attacks.

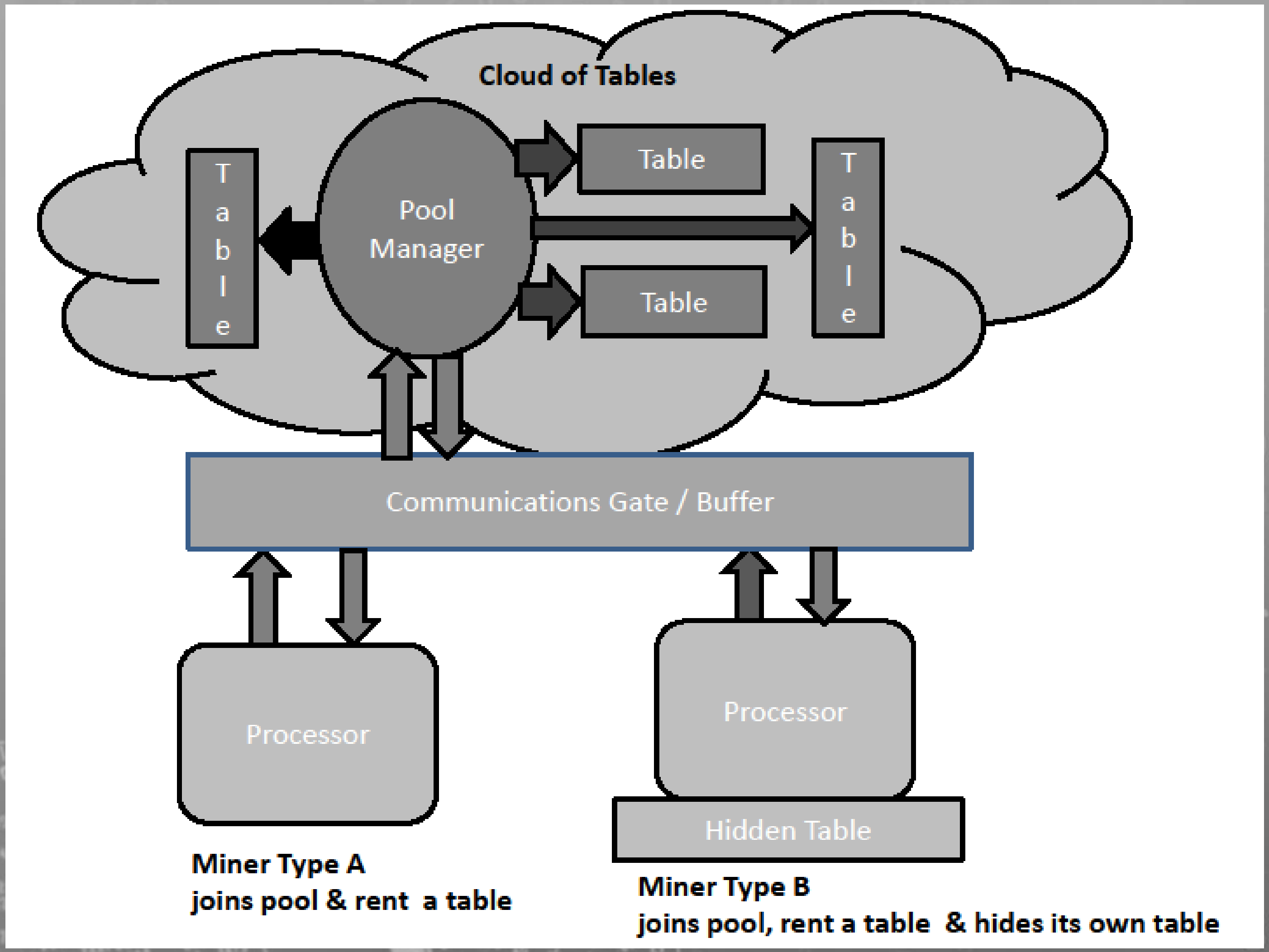
Machine Learning & Game Theory

- Deep learning is a fast-evolving area for research in the domain of artificial intelligence.
- Game theory has been showing its multi-dimensional applications in the last few decades.
- Game theory helps to model or solve various deep learning-based problems and game theory is a potential approach to improve results in deep learning models.
- Accordingly, the design of deep learning models often involves a game-theoretic approach.

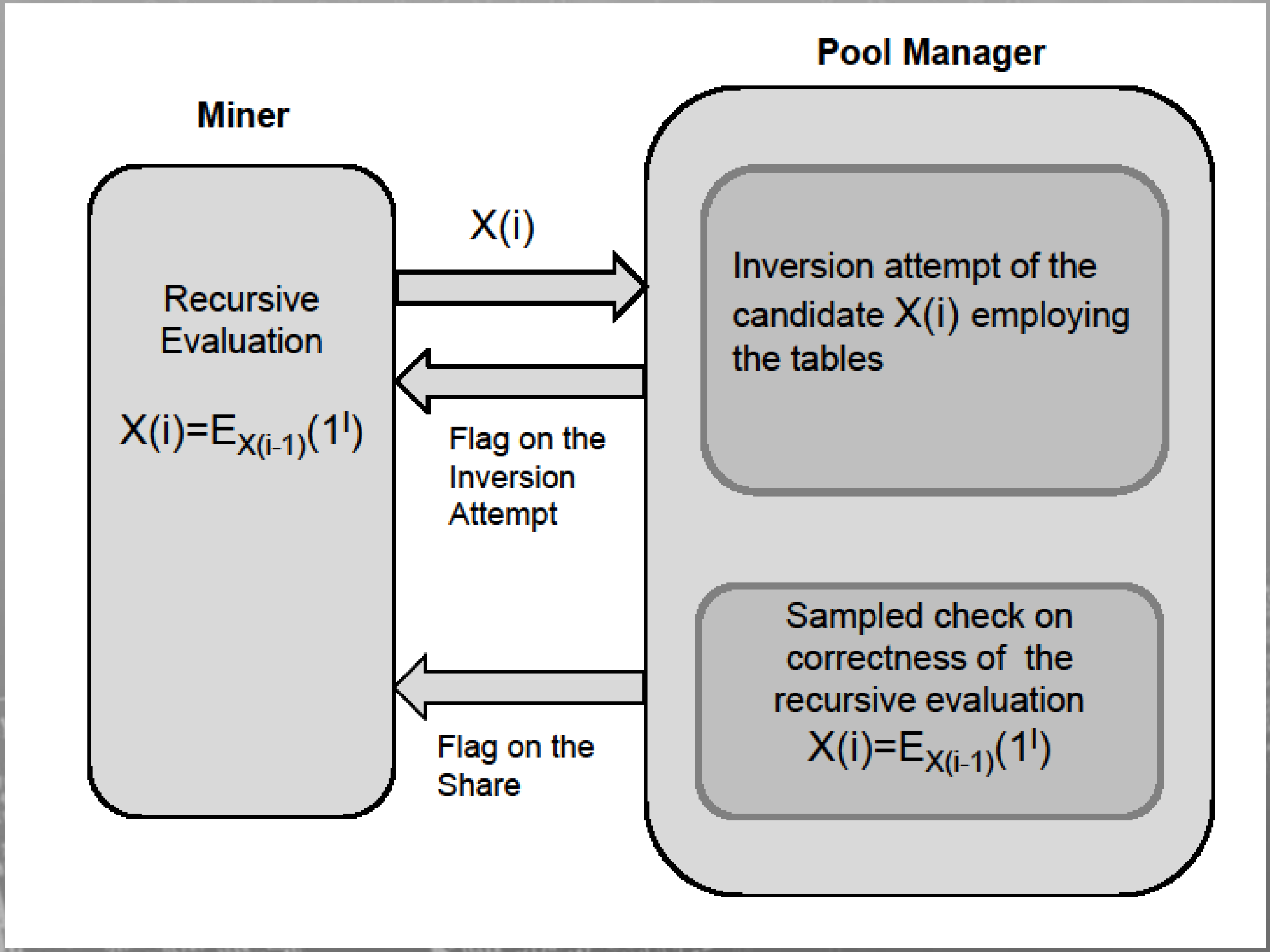
- Miners could exhibit malicious behaviors which cause a waste of distributed computation resource, even posing a threat on the efficiency of blockchain networks.
- A reputation-based mechanism could be employed for the PoW miners in the blockchain, in which miners are incentivized to conduct honest mining.
- Based on the game theory, reputation-based algorithm have been proposed to encourage honest mining of miners, and thereby increase the overall revenue of the pool.

OUR ALTERNATIVE: POOL MINING ARCHITECTURE RESISTANT AGAINST DISHONEST MINERS

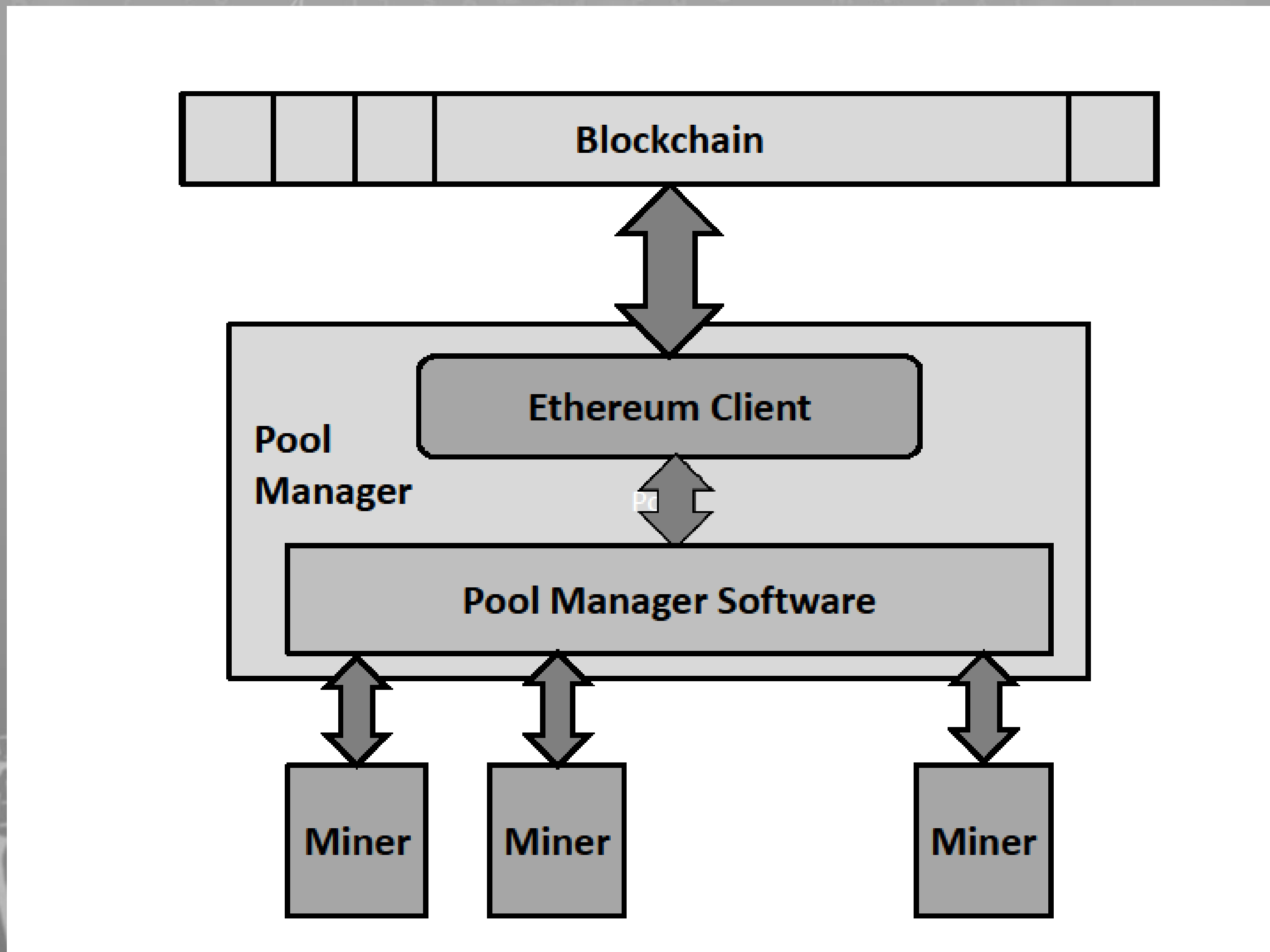
Architecture of the proposed pool mining



Interaction of a miner and pool manager during the puzzle solving process



Architecture of the implemented mining pool



3. PRIVACY EVALUATION OF CERTAIN BC LEDGERS EMPLOYING TECHNIQUES OF AI

Identity privacy attack

- In an identity privacy attack, an attacker obtains user privacy information using the connection between the trader's address on the chain and the user's real identity.
- The attacker infers a user's identity by monitoring public data in the global ledger and analyses related transactions between addresses.
- Presently, common identity privacy attack mainly includes the key, replay, and impersonation attacks.

Key attack

- It occurs when an attacker illegally obtains a private key. Key attacks are performed using software and physical methods.
- In software methods, an attacker uses specific malicious software to obtain private key data from a cryptographic software system to steal the user’s privacy information.
- In physical methods, an attacker directly steals the connection between the user’s real identity and the trader’s address on the chain and obtains the privacy information of the transaction participants using the transaction associated graph.

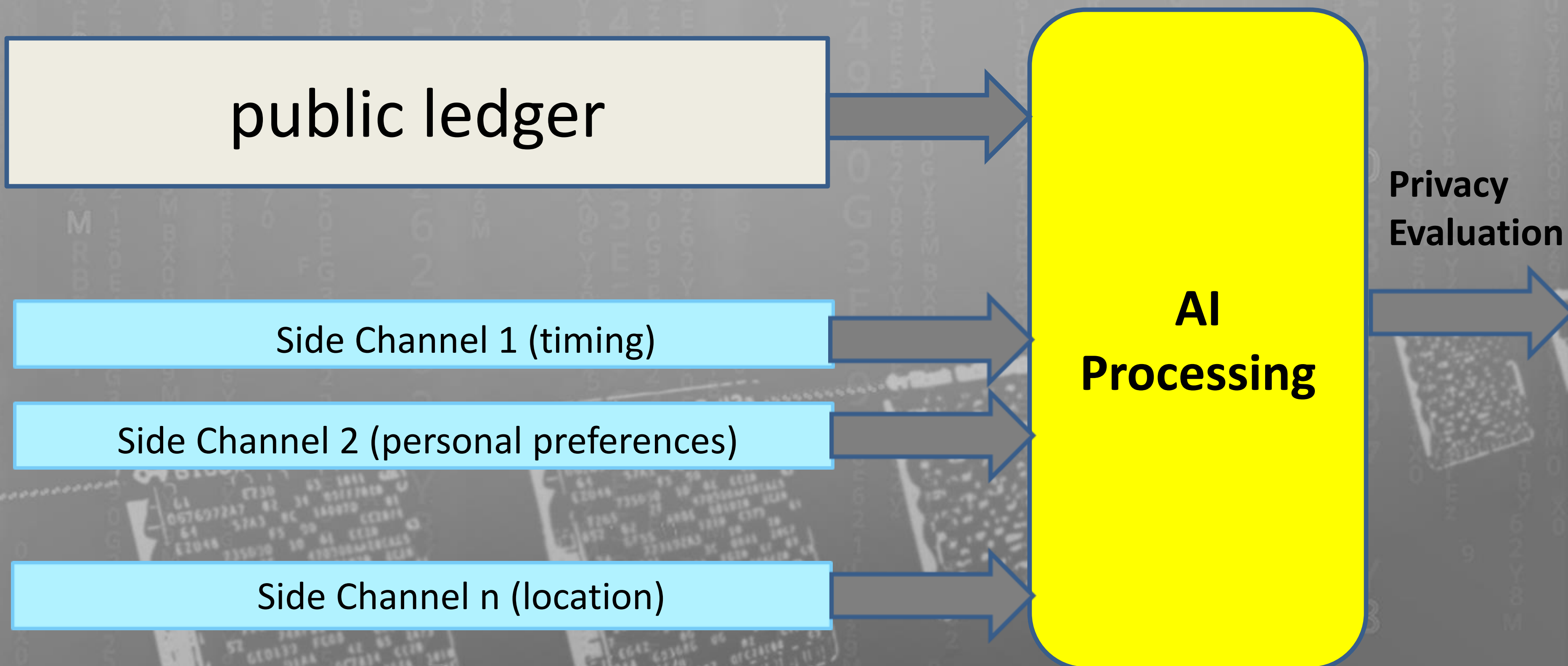
Replay attack

- It occurs when an attacker intercepts the user’s trans- action data and sends a packet received by the destination host, thereby damaging the authentication of the user identity.
- Because the blockchain generates a private key during the signing process, an attacker combines the private key information to launch a replay attack, thus affecting the signing process of the blockchain.

Impersonation attack

- Impersonation attack: It occurs when the attacker pretends to be a legitimate user to perform unauthorized operations.
- In the transaction process, an attacker impersonates both parties of the transaction and simulates the exchange to steal privacy information.
- Once an attacker successfully fakes the identity of legitimate users, the user’s privacy information is greatly threatened.

Our Approach: Public Ledger Privacy Evaluation Employing Side Channel Information and AI Techniques



The machine learning approaches

- **Support Vector Machine (SVM)**: It is a supervised machine learning method. It separates the classes with a hyper-plane, which maximizes the margin between classes.
- **C4.5**: It is used to classify the data using a decision tree. C4.5 algorithm is developed based on the ID3 (Iterative Dichotomiser) algorithm
- **KNN (k-Nearest Neighbours)**: KNN algorithm first takes k nearest training samples as a testing data set, and then it predicts the sample data set with major class among the testing data set. In the selection of k nearest neighbours, KNN needs to compute the distance of all training samples for each test sample. It costs more linear time complexity, which is why it not being used for big data applications. Challenge for the KNN algorithm is that it has the same impact on all features and characteristics during the classification, even if some characteristics are less important. As a result, it may deviate the classification and decrease the efficiency of the algorithm.
- **MLP (Multilayer Perceptron)**: It is a neural network methodology where a hidden layer is added in between the input and output layer. The supervisory learning is performed with backpropagation algorithm, which classifies linearly non-separable data.

Фонд за науку
Републике Србије

THANK YOU VERY MUCH FOR THE ATTENTION