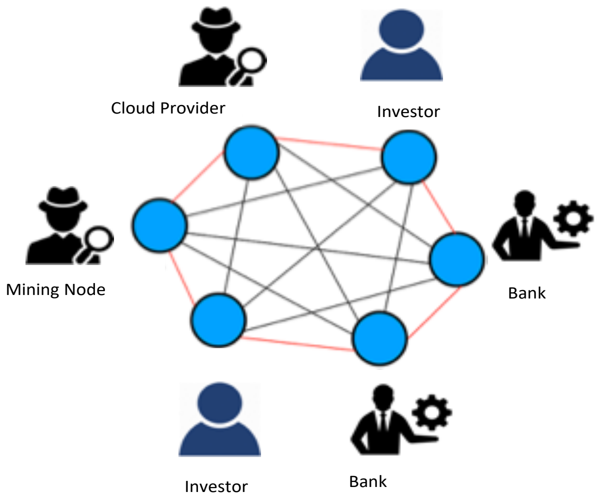
Scan this to download the slides



A Reputation Management Framework for Knowledge-Based and Probabilistic Blockchains

Tara Salman, Raj Jain, Lav Gupta

Washington University in St. Louis

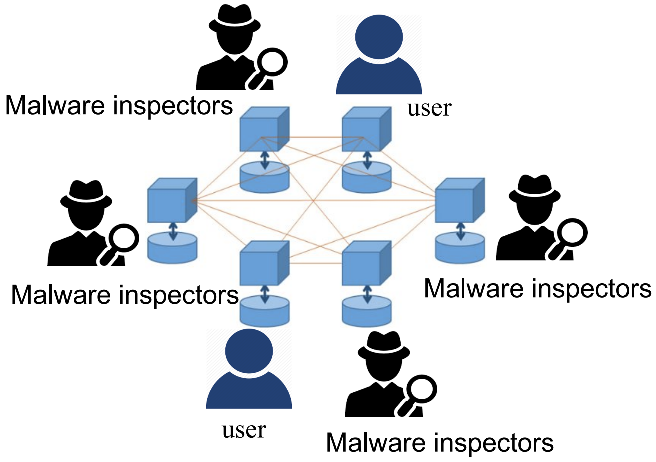
Tara Salman, Raj Jain, and Lav Gupta, "**A Reputation Management Framework for Knowledge-Based and Probabilistic Blockchains**," IEEE 1st International Workshop on Advances in Artificial Intelligence for Blockchain (AIChain 2019), held in conjunction with the 2019 IEEE International Conference on Blockchain, Atlanta, July 14, 2019, http://www.cse.wustl.edu/~jain/papers/rpmcewa.htm.

Outline

- Knowledge-based and probabilistic blockchains
- Reputation management requirements
- Our approach
- Application to malicious node detection
- Limitations and work extensions

Blockchains and Knowledge-based Blockchain

- Blockchains are distributed, secure, and immutable systems
- Getting popular in building distributed AI and decision making applications → ***Knowledge-based blockchains***
  - Transform the chain from a data storage to a processing and decision making platform
- Example: Malware detection system
  - Multiple malware inspectors analyze a file submitted by a user. The blockchain returns a "consensus" decision about that malware



A malware detection system example

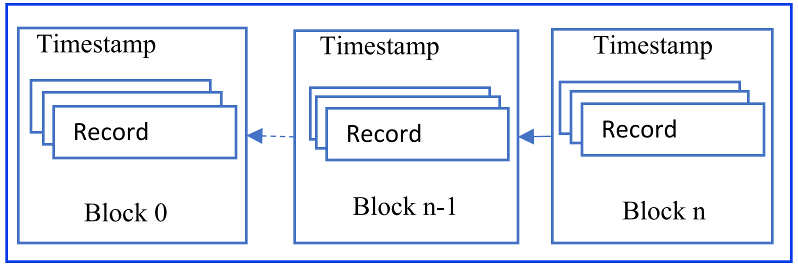
Need for Blockchain Extensions

- Knowledge-based blockchains require:
  1. Transactions → store probabilistic decisions
  2. Blockchains should be able to summarize decisions and achieve consensus
  3. Consensuses should be visible to others and possibly updated whenever needed
- Challenge
  - Current blockchain systems cannot efficiently do that
- Solution:
  - Extend blockchain systems to meet these requirements

  → ***probabilistic blockchain***

Probabilistic Blockchain

Traditional chain

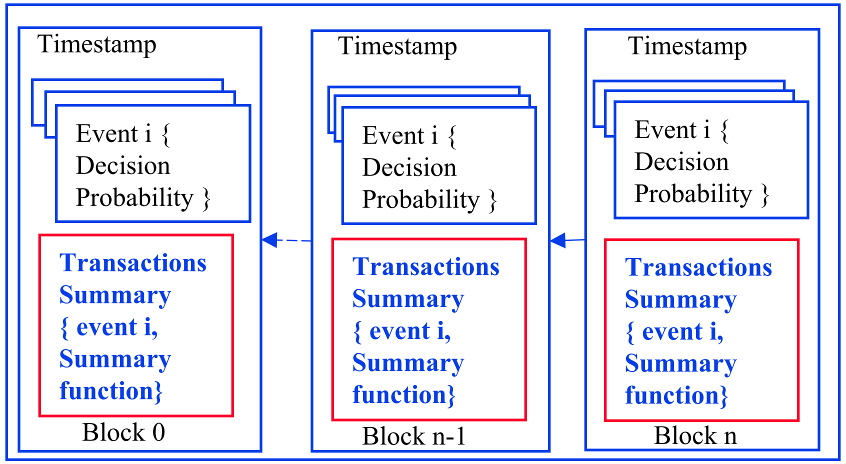


Users broadcast transactions or contracts (Records)

Miners validate transactions and generate blocks

Blockchain nodes validate the block and construct the chain

Probabilistic chain



Users broadcast transactions (**Decisions/opinions**)

Miners validate transactions, **create a knowledgeable summary** and generate blocks

Blockchain nodes validate the block and construct the chain

Tara Salman, Raj Jain, and Lav Gupta, "**Probabilistic Blockchains: A Blockchain Paradigm for Collaborative Decision-Making**," 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON 2018), New York, NY, November 8-10, 2018, 9 pp., http://www.cse.wustl.edu/~jain/papers/pbc_uem.htm

The Need for Agent Reputation Framework

- The challenge is that not all agents contributing to the group decision may be treated equally
  - Agents contribution to the collaborative decision should be based on their past performance

- **A reputation management framework is needed** to assign reputations to agents
  - Good decisions → Reputation close to 1
  - Bad decisions → Reputation close to 0
  - Just starting → Reputation is 0.5

Reputation Function Requirements

1. **Time-dependent**
   - A mistake in the past should not be treated the same as a recent one

2. **Configurable increase and decrease**
   - Suit different applications

3. **Proportional update**
   - The decrease after a wrong decision is proportional to how good an agent has performed so far; thus, provide fairness

Reputation Function

- Our work extends Exponentially Weighted Average function (EWA) to Rated Proportional Multi-Configurable EWA (RPMC-EWA)

- EWA does not meet configurable increase and decrease and proportional update

$$R_{i,t} = \begin{cases} 0 & t = 0 \\ \alpha X + (1-\alpha) R_{i,t-1} & t \neq 0 \end{cases}$$

EWA

- ***p*** is the number of correct decisions, ***n*** is the number of wrong decisions before time *t*, ***α*** is configurable increase, ***β*** configurable decrease

$$R_t = \frac{\begin{cases} 0 & p=0,\ n=0,\ t=0 \\ \alpha \frac{p}{p+n} + (1-\alpha)(2R_{t-1}-1) & t>0,\ \text{correct decision} \\ \beta \frac{-n}{p+n} + (1-\beta)(2R_{t-1}-1) & t>0,\ \text{wrong decision} \end{cases}}{2} + 0.5$$

RPMC-EWA

Reputations in Probabilistic Blockchains

- How it is done?
  - Miner get latest reputations and use it for calculating the consensus
  - Validators recalculate the consensus with their latest reputations and use it for validating
  - Everyone update the reputation value based on the last decision made

- Applications
  - Malicious node detection
  - Efficient collaborative decision approach

Application to Malicious Node Detection

- Evaluate the effect of malicious node detection on the collaborative decision in probabilistic blockchains
  - Summary function for probabilistic blockchains: mean

- Setup:
  - Ten agents are participating with one malicious.
  - Honest nodes give 1 as a decision while a malicious node flips the decision.

- Metric:
  - When the consensus decision return back to 1 (i.e., malicious node with a reputation of less than 0.5 is eliminated)

Malicious Node Strategies

- **Continuous-flipping strategy**

Non malicious decisions → malicious decisions

Non malicious decisions		malicious decisions	
1 1 1 1 1 1 1 1 1 1	→	0 0 0 0 0 0 0 0 0 0	Flip all

- **Pattern-flipping strategy**

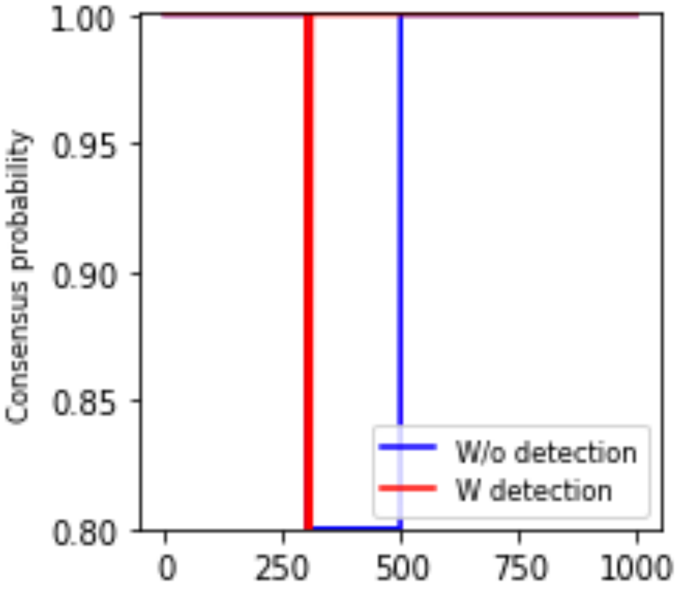
Non malicious decisions		malicious decisions	
1 1 1 1 1 1 1 1 1 1	→	0 0 0 1 0 0 0 1 0 0	Flip Every 4th

- **Random-flipping strategy**

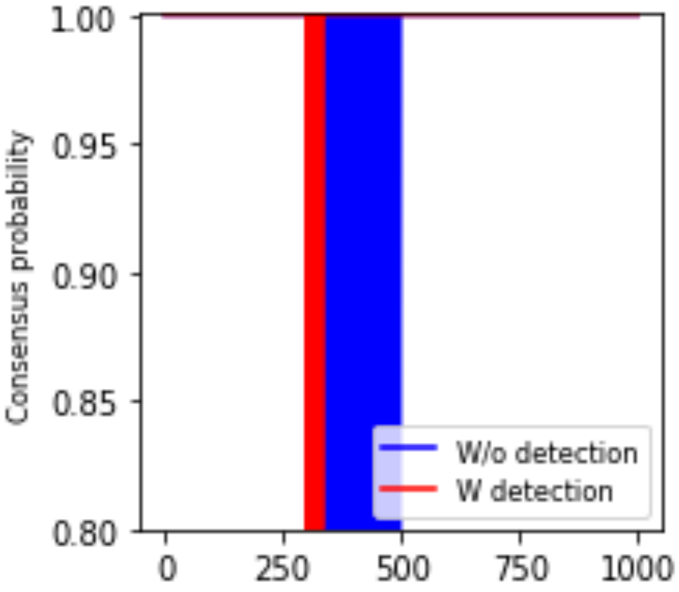
Non malicious decisions		malicious decisions	
1 1 1 1 1 1 1 1 1 1	→	0 0 0 1 0 1 0 0 1 0	Flip Randomly

Results

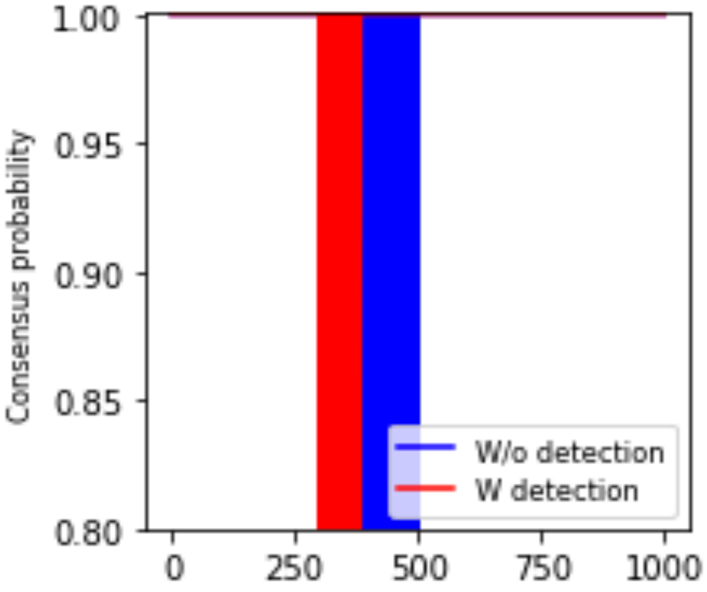
A node turned malicious from decision 300 to decision 500



Continuous flipping
RPMC-EWA has recovered after less than 10 decisions



Random flipping
RPMC-EWA has recovered after 25 decisions



Pattern flipping
RPMC-EWA has recovered after 50 decisions

Limitations and Further Extensions

- Limitation 1: Empirical analysis (off-chain)
  - The reputation framework integration with a blockchain platform
- Limitation 2: The framework security, computation, and overhead analyses are not considered
  - Effects of consensus and reputation calculation on throughput and delay should be measured
  - Theoretical and practical security analyses need to be considered

Conclusion

- Probabilistic blockchains transform blockchains from data storage to data analyses and processing engine
- A reputation management framework is essential for better decision making and malicious node detection
- This work proposed as an extension of EWA that meets our requirements of reputation functions
- Empirical validations showed that the proposed approach outperform the baselines
- Extensions include implementation, and proper security and performance analyses

Scan QR code to download the slides

Tara Salman
Tara.salman@wustl.edu
https://sites.wustl.edu/tarasalman/