Kuwait Journal of Science, Vol.49, No.(1), January.2022

A resilient Micro-payment Infrastructure: an approach based on Blockchain technology

Soumaya Bel Hadj Youssef

Pr. Noureddine Boudriga

Context & Motivations

❖ Micro-payment systems constitute an attractive solution and provides many advantages for the customers and merchants.

Gap: The proposed micro-payment systems that are not based on BC technology still need for more security, higher efficiency, and better reactivity.

The Blockchain (BC) technology can be a promising solution for micropayment systems.

Gap: In the proposed micro-payment systems based on the BC technology:

- No assessment of the risk of loss.
- No attention to the behaviour of the user.
- No adaptation of the response time of the BC network to the user's trust level.
- No resilience and robustness to the transaction processing.

Objective

Proposition of trust-aware and resilient micro-payment infrastructure based on BC technology and an auditor:

- ✓ detect misbehaving users and attacks.
- ✓ provide robustness through the analyze of the risk of loss.
- ✓ reduce the verification delay and user waiting time.
- ✓ control the block size in the blockchain network.
- ✓ diminish the risk of loss related to false micro-payment.
- ✓ respond to attacks in a fast and effective manner.

Contributions

1. Proposition of a resilient micro-payment infrastructure using the BC technology and an auditor.
2. Provision of three user’s trust models.
3. Building a function that adapts the size of block to be transmitted to the BC network to the user’s trust level and the willingness of the auditor to take a risk.
4. Provision of the validation of the micro-payment infrastructure.

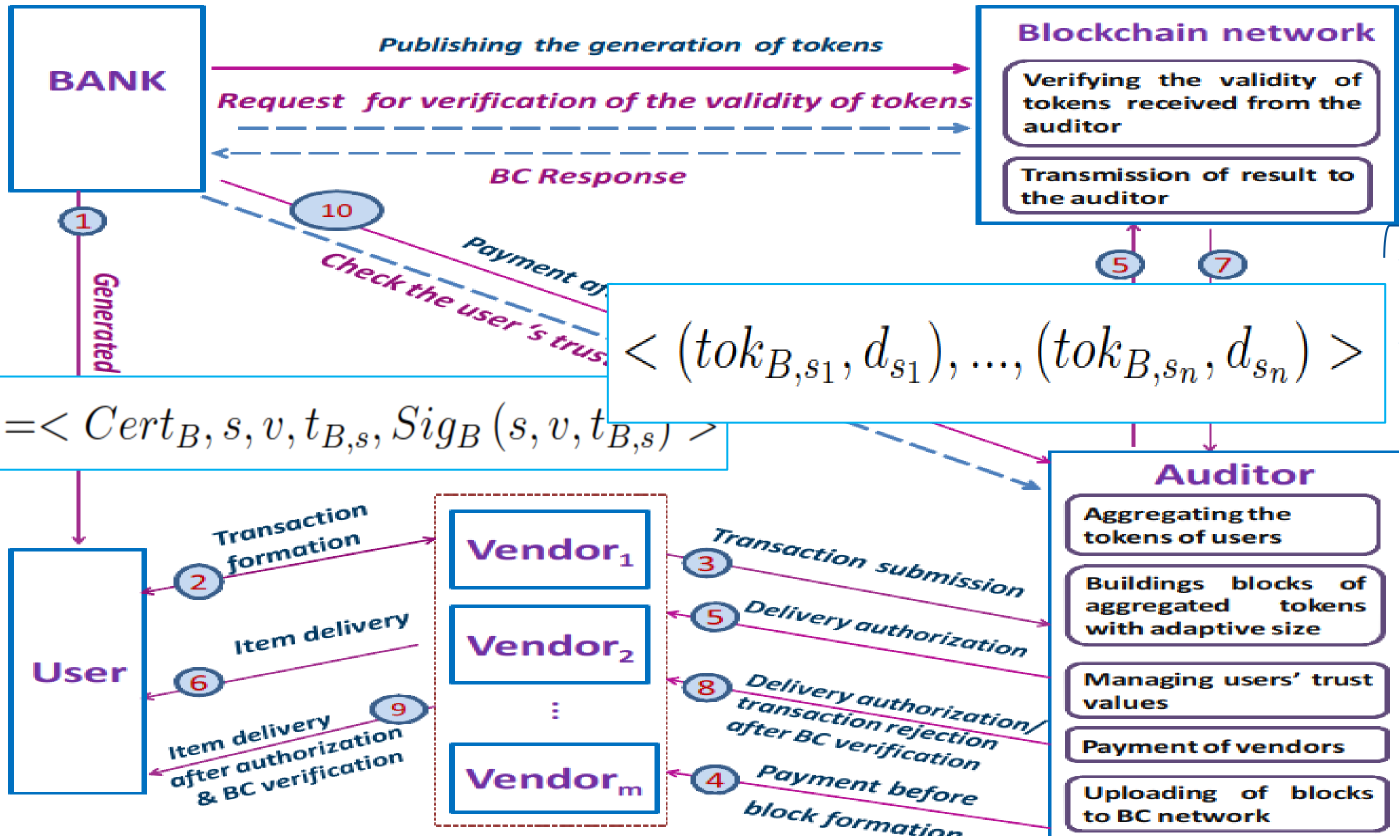
OUTLINE

1. Requirements for a resilient micro-payment infrastructure
2. Micro-payment infrastructure
3. User's Trust models and and auditor's decision
4. Risk assessment
5. Infrastructure validation
6. Simulation & Results
7. Conclusion & Perspectives

Requirements for a resilient micro-payment infrastructure

- ❖ Tokens aggregation
- ❖ Double-spending prevention
- ❖ Double-selling prevention
- ❖ Tokens forging attack prevention
- ❖ Authentication of payment transaction
- ❖ Payment transaction tracing
- ❖ Actors’ trust management

Micro-payment infrastructure



$$< (tok_{B,s_1}, d_{s_1}), \ldots, (tok_{B,s_n}, d_{s_n}) >$$

$$tok_{B,s} =< Cert_B, s, v, t_{B,s}, Sig_B(s, v, t_{B,s}) >$$

d_{si}

11: token is valid
01: token is altered
10: token is duplicate
00: token does'nt occure in bank publication

$$Tr_{u,m,t} =< Cert_u, Cert_m, t, TOK, INF, Sig_m(Sig_u(t, TOK, INF)) >$$

t: time of transaction creation, INF: information about the item,
TOK: set of tokens covering the price of item to buy

Micro-payment infrastructure (2)

Token reimbursement and transaction payment

Two situations:

- ✓ Block under building (not reached size)
  - \- Merchant proceeds with the item delivery
  - \- Auditor redeems all the tokens in the transaction

➡ The merchant receives : $size(tr) \times (v - \rho)$

Number of tokens in the transaction (size(tr)) ***Token value*** (v) ***Value compensating auditor risk*** (ρ)

- ✓ Block under verification (reached size)

Merchant must wait for the block validation:

- Valid block ➡ transaction is accepted and the merchant receives $size(tr) \times (v - \rho)$
- <u>One invalid</u> token ➡ transaction is rejected and no item is received by the buyer.

<u>Result of BC</u> : l invalid tokens in a block and l_o tokens occur in tr.

➡ Auditor will lose an amount $(l - l_0) \times (v - \rho)$

User trust models and auditor's decision (1)

Trust computation:

1. The auditor selects an initial value of the block size **Wo** depending on the information delivered by the bank, the profile of the user, and the experience of auditor.
2. It computes the initial trust value assigned to the user.
3. The user's trust value will be recomputed after reception of each result related to the submission of a block to the BC network.

Main idea : punish the dishonest users by reducing the block size, while encouraging the honest users.

➡ User trust is dynamic and depends on the risk of loss.

User trust models and auditor's decision (2)

✓ **Neutral profile** is expressed by a linear trust function, computed according to the beta distribution E (beta (α + 1, β + 1))

$$T_0\left(\beta_i\right) = \frac{\left(W_{i-1} - \beta_i\right) + 1}{W_{i-1} + 2}$$

W_i: size of block B_i

W_{i-1}: size of block B_{i-1}

α: number of valid tokens

β: number of invalid tokens

✓ **Optimistic profile** is expressed by an exponential trust function:

$$T_1\left(\beta_i\right) = 1 - \gamma_2 \times \exp\left(-\delta_2 \times \left(W_{i-1} - \beta_i\right)\right)$$

$$\gamma_2 = \frac{W_{i-1}+1}{W_{i-1}+2}$$

$$\delta_2 = \frac{\log(1+W_{i-1})}{W_{i-1}}$$

✓ **Pessimistic profile** is expressed by an exponential trust function:

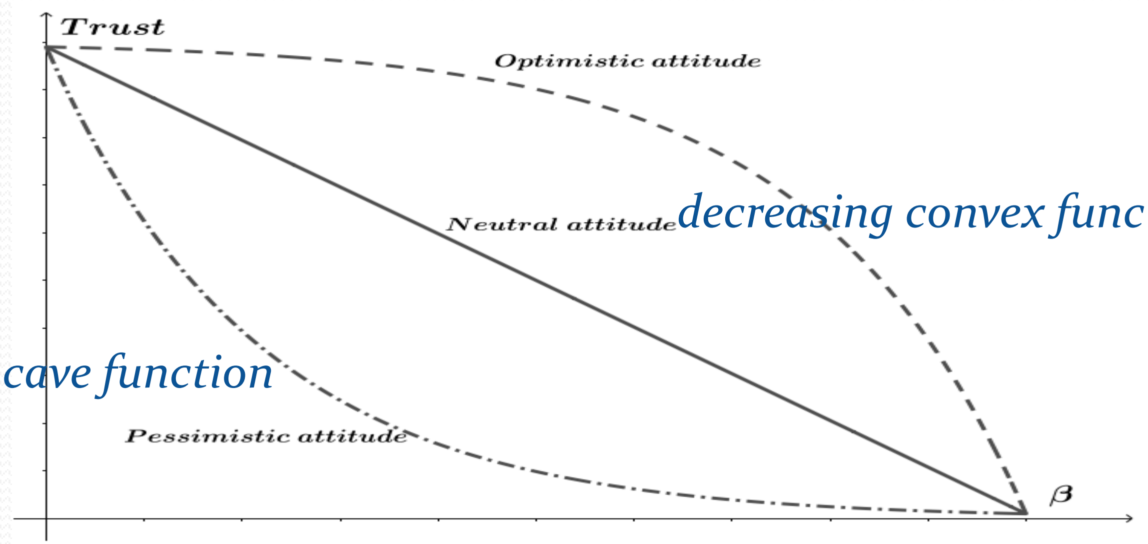
$$T_2\left(\beta_i\right) = \gamma_1 \times \exp\left(\delta_1 \times \left(W_{i-1} - \beta_i\right)\right)$$

$$\gamma_1 = \frac{1}{W_{i-1}+2}$$

$$\delta_1 = \frac{\log(1+W_{i-1}}{W_{i-1}})$$

User trust models and auditor’s decision (3)

- ✓ **Optimistic model**: the user’s trust decreases slowly with the increase of β.
- ✓ **Pessimistic model**: the user’s trust decreases rapidly with the increase of β.
- ✓ **Neutral model**: the user’s trust decreases linearly with the increase of β.



$$\forall \beta : T_2(\beta) \le T_0(\beta) \le T_1(\beta)$$

The three models have the same start and end points.

$$T_0(\beta=0) = T_1(\beta=0) = T_2(\beta=0) = \frac{W_0+1}{W_0+2} \qquad T_0(\beta=W) = T_1(\beta=W) = T_2(\beta=W) = \frac{1}{W+2}$$

User trust models and auditor's decision (4)

Size of the i(th) block:

$$\frac{T_e(\gamma_i) - T_e(\gamma_{i-1})}{T_e(\gamma_{i-1})} = \frac{x_i - W_{i-1,u}}{W_{i-1,u}}$$

$\gamma_i = \sum_{j=1}^{i} \beta_j$: sum of the number of invalid tokens in the previous blocks

T_e: user profile

The Block size changes over time according to the user's profile.

Risk assessment

- ✓ The risk is the possibility that the auditor loses money due to the increase of the number of invalid tokens in the different blocks.
- ✓ Risk value is the difference between the amount of payment made to the merchant and the amount received from the bank for the valid tokens in a block.
- ✓ After validation result of the (n)th block:

Valid block :

$$Rsk_{n,u} = W_{n-1,u}v(1-\rho) - W_{n-1,u}v = -W_{n-1,u}v\rho$$

Invalid block : the auditor rejects the transaction:

$$Rsk_{n,u} = \sum_{i \leq p-1} | tr_{n,i} | v(1-\rho) - \sum_{i \leq p-1} (| tr_i | - \beta_{n,u,i})v$$

Amount paid to the merchant *Amount received from the bank*

$| tr_i |$: number of tokens in transaction tr_i.

$\beta_{n,u,1}, \ldots, \beta_{n,u,p-1}$ number of invalid tokens in $tr_1, \ldots, tr_p$

Infrastructure validation

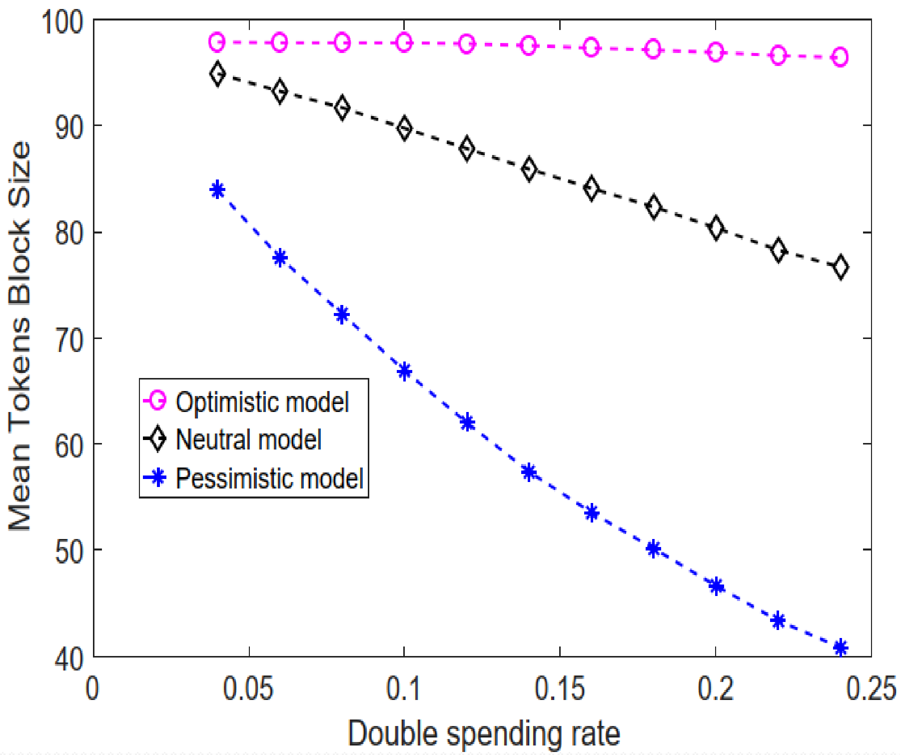
- **Prevention from double-spending** by identifying each token by a unique identity and adding the certificates of all the actors.
- **Prevention from double-selling** by adding the certificates of all the actors and including information about the purchase.
- **Prevention from Tokens forging** by including the certificates of actors and providing the signature mechanism.
- **Payment tracing** through the use of BC technology and timestamps.
- **Actors' trust management** through the use of an auditor which computes the user's trust value.
- **Overhead reduction :**

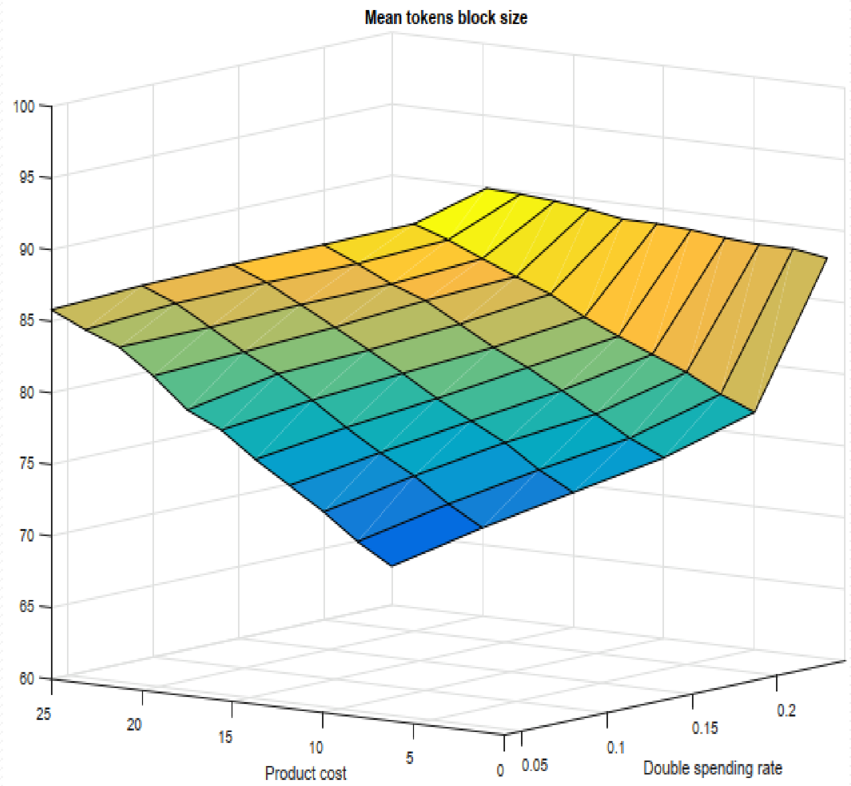
- in terms of communication and cost (reduction of number of messages transmitted towards the blockchain).

- in terms of processing: at the vendor (aggregation of tokens), at the auditor (reduction of number of verifications), and at blockchain network (less reception of transactions).

Simulation and results (1)

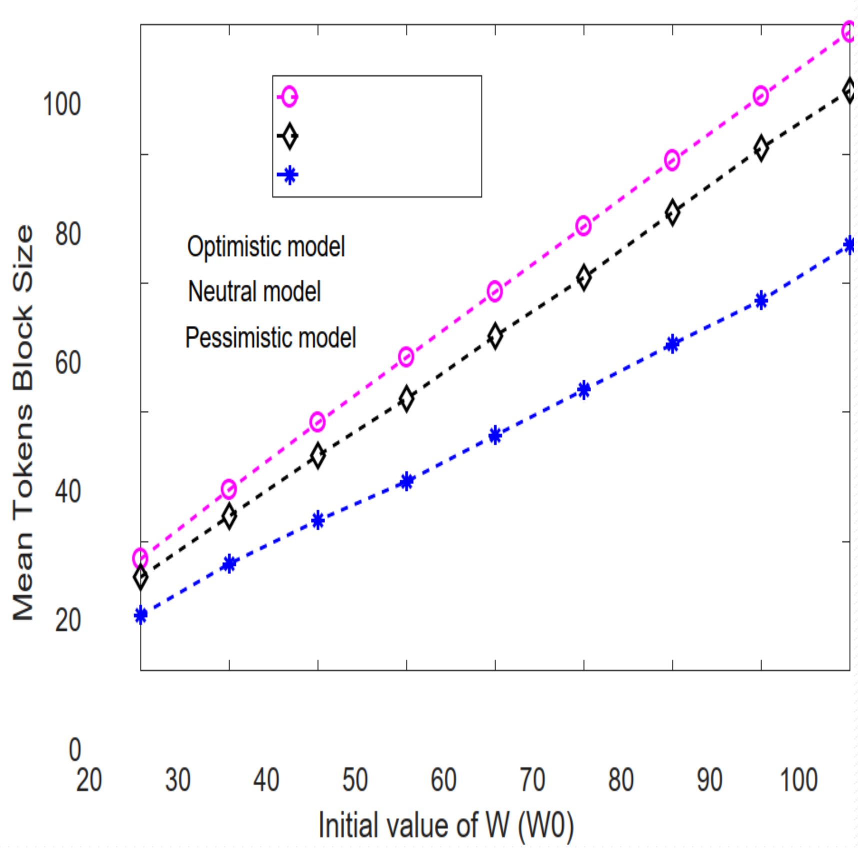
Mean Tokens Block Size w.r.t Generation rate of double spending tokens

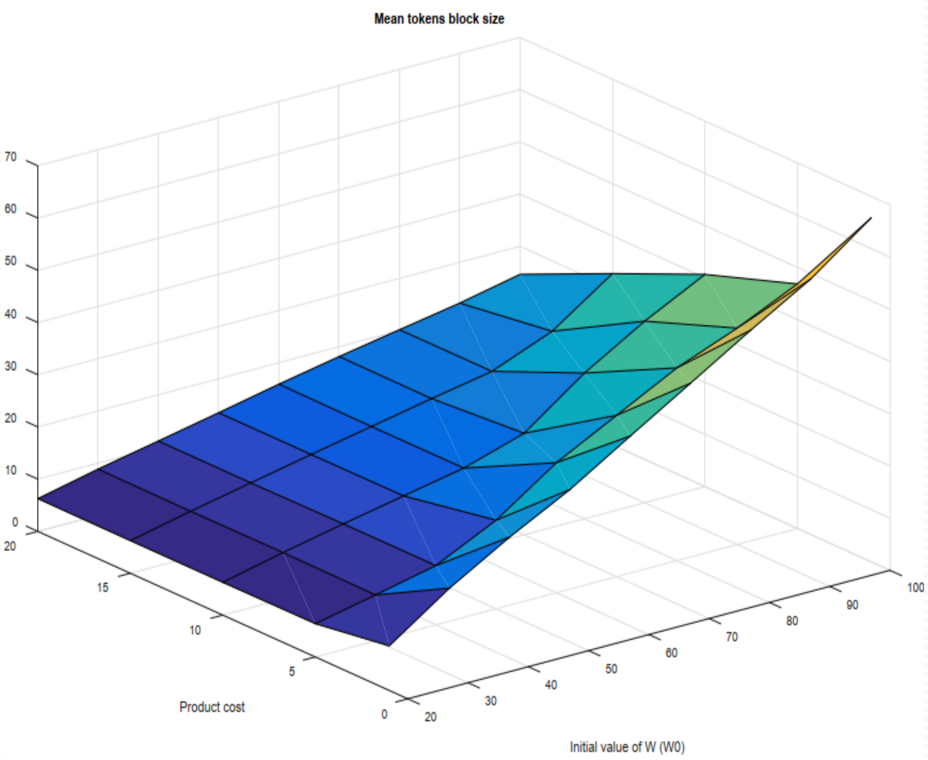




Simulation and results (2)

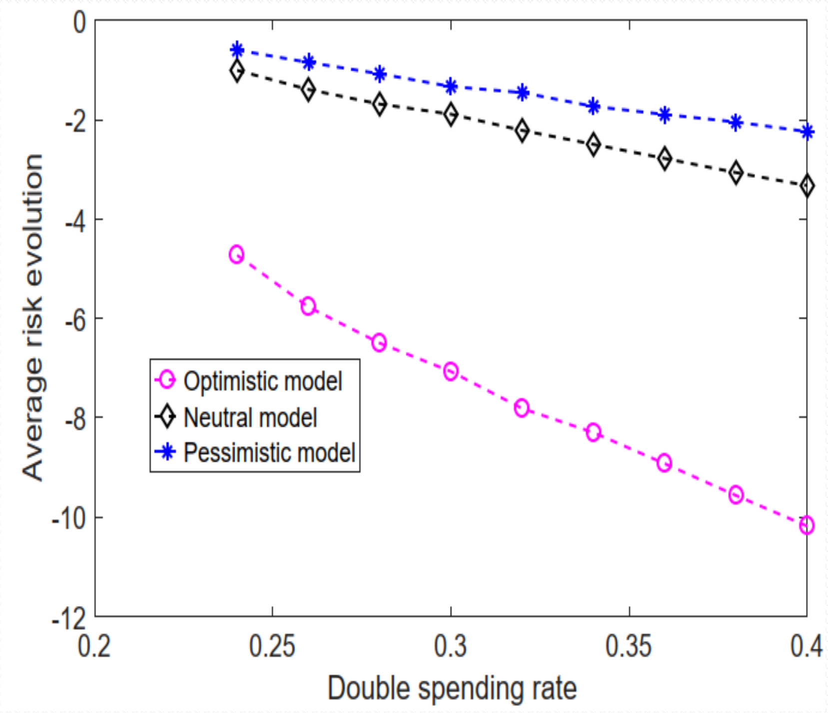
Mean Tokens Block Size w.r.t Initial value of W



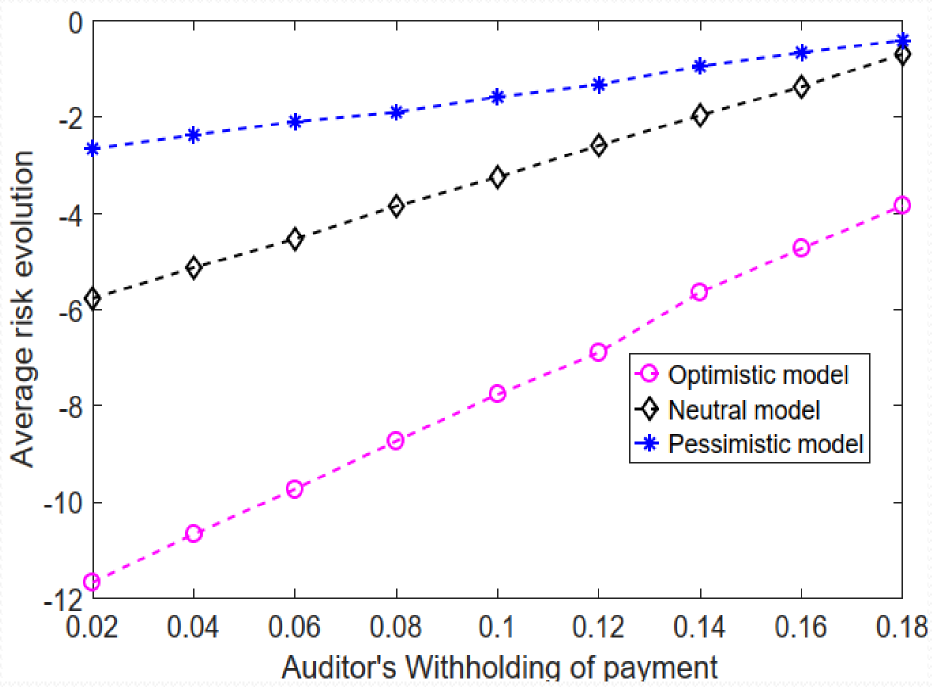


Simulation and results (3)

Average risk evolution w.r.t Generation rate of double spending tokens



Average risk evolution w.r.t Auditor's withholding of payment



Conclusion and perspectives

Conclusion

- We presented a resilient micro-payment infrastructure.
- We proposed three trust models for computing the trust values of the user.
- We presented the decision made by the auditor and we assessed the risk.
- We validated our micro-payment infrastructure and analyzed the performance of our proposed trust models.

Perspectives

- Showing the scalability of our infrastructure by considering many buyers and sellers.
- Using two or more auditors and showing their impact on the performance of our micropayment infrastructure.

THANK YOU

for your attention