PAYMENT PROJECT

Principal Investigator: Pro. Steven Murdoch

Research Fellow: Aydin Abadi

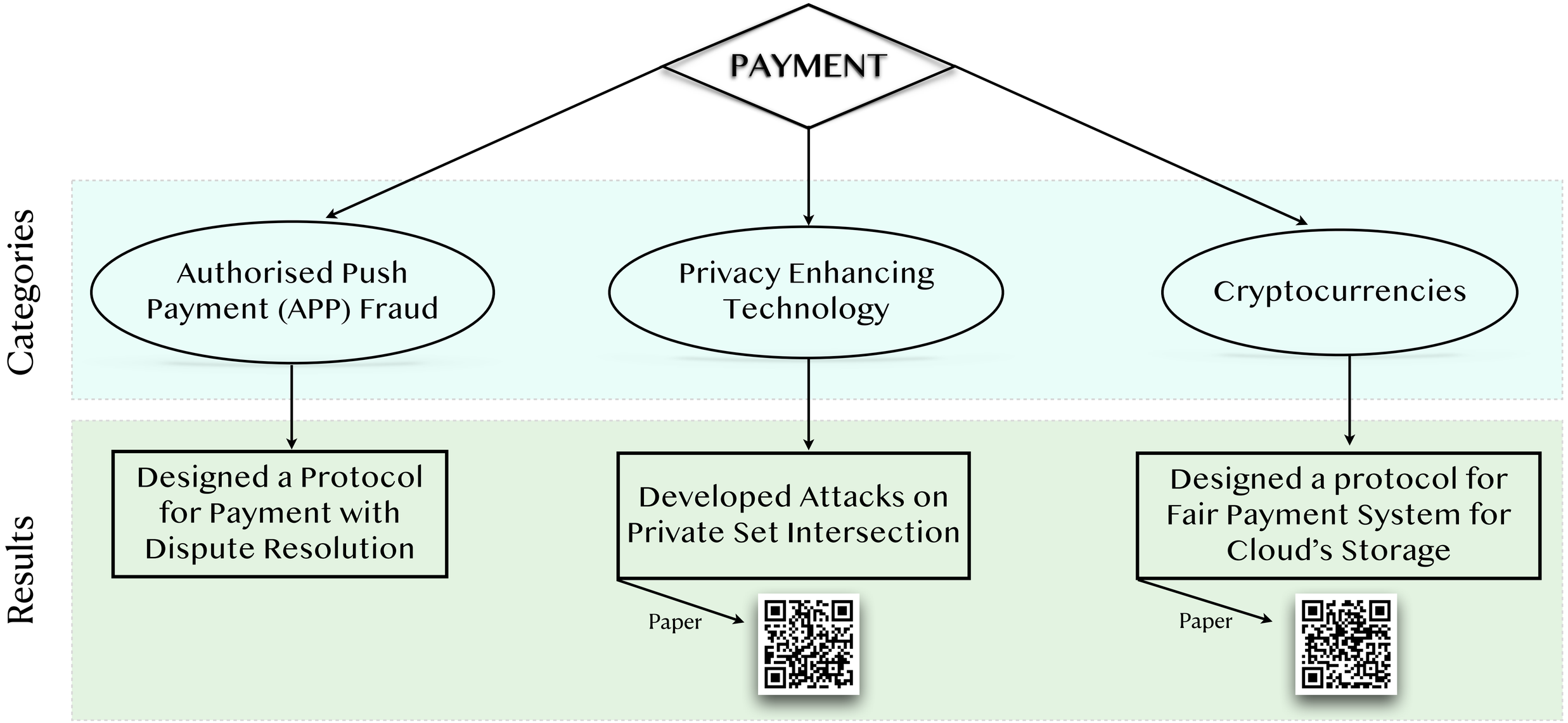
UCL

National Research Centre on
Privacy, Harm Reduction
and Adversarial Influence
Online

PAYMENT PROJECT

Progress so far

REPHRAIN
Protecting citizens online



PAYMENT PROJECT

Authorised Push Payment (APP) Fraud

Background

- ‘’Authorised Push Payment” (APP) fraud:
  - Definition: An APP fraud is a type of cyber-crime where a fraudster tricks a victim into making an authorised online payment into an account controlled by the fraudster.
  - It is called “authorised” because the victim authorises the payment.
  - The APP fraud has various variants, such as:
    - romance
    - investment
    - CEO
    - invoice

PAYMENT PROJECT

Authorised Push Payment (APP) Fraud

Background

- The amount of money lost due to APP frauds is substantial
    - Only in the first half of 2021, a total of £355 million was lost to APP frauds.
- APP fraud is a global issue.
    - According to the **FBI**'s report, victims of APP frauds reported at least a total of $419 million losses, in 2020.
    - Recently, **Interpol** warned its member countries about a concerning variant of APP fraud called investment fraud via dating software.

PAYMENT PROJECT

Authorised Push Payment (APP) Fraud

Problem

- Although the UK's regulators (unlike other countries) have provided specific guidelines to financial institutes to prevent APP frauds occurrence and improve victims' protection, these guidelines are:
    - ambiguous
    - open to interpretation
- Also, there exists no mechanism in place via which honest victims can prove their innocence.

National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online

PAYMENT PROJECT

Authorised Push Payment (APP) Fraud

REPHRAIN Protecting citizens online

Our Solution

- To protect victims of APP frauds, we proposed:
  1. **Formal Definition:** we put forward the notion of "Payment with Dispute Resolution" (PwDR):
     - Identified a PwDR scheme's core security properties:
       1. security against a malicious victim.
       2. security against a malicious bank.
       3. privacy.
     - formally defined the PwDR scheme.

Security Game

$$\texttt{keyGen}(1^\lambda) \rightarrow (sk, pk)$$
$$\texttt{bankInit}(1^\lambda) \rightarrow (T, pp, \boldsymbol{l})$$
$$\mathcal{A}(1^\lambda, T, pp, \boldsymbol{l}) \rightarrow \hat{m}_1^{(\mathcal{C})}$$
$$\texttt{insertNewPayee}(\hat{m}_1^{(\mathcal{C})}, \boldsymbol{l}) \rightarrow \hat{\boldsymbol{l}}$$
$$\texttt{genWarning}(T, \hat{\boldsymbol{l}}, \text{aux}) \rightarrow \hat{m}_1^{(\mathcal{B})}$$
$$\mathcal{A}(T, \hat{\boldsymbol{l}}, \hat{m}_1^{(\mathcal{B})}) \rightarrow \hat{m}_2^{(\mathcal{C})}$$
$$\texttt{makePayment}(T, \hat{m}_2^{(\mathcal{C})}) \rightarrow \hat{m}_2^{(\mathcal{B})}$$
$$\mathcal{A}(\hat{m}_1^{(\mathcal{B})}, \hat{m}_2^{(\mathcal{B})}, T, pk) \rightarrow (\hat{z}, \hat{\ddot{\pi}})$$
$$\forall j, j \in [n]:$$
$$\left(\texttt{verComplaint}(\hat{z}, \hat{\ddot{\pi}}, g, \hat{\boldsymbol{m}}, \hat{\boldsymbol{l}}, j, sk_{\mathcal{D}}, aux, pp) \rightarrow \hat{\boldsymbol{w}}_j\right)$$
$$\texttt{resDispute}(T_2, \hat{\boldsymbol{w}}, pp) \rightarrow \boldsymbol{v} = [v_1, ..., v_4]$$

Adversary's wining probability

$$\Pr\left[\begin{array}{l} \left((m_1^{(\mathcal{B})} = warning) \wedge (\sum_{j=1}^{n} w_{1,j} \geq e)\right) \\ \vee\left((\sum_{j=1}^{n} w_{1,j} < e) \wedge (v_1 = 1)\right) \\ \vee\left((\texttt{checkWarning}(m_1^{(\mathcal{B})}) = 1) \wedge (\sum_{j=1}^{n} w_{2,j} \geq e)\right) \\ \vee\left((\sum_{j=1}^{n} w_{2,j} < e) \wedge (v_2 = 1)\right) \\ \vee\left(u \notin Q \wedge \texttt{Sig.ver}(pk, u, sig) = 1\right) \\ \vee\left((\sum_{j=1}^{n} w_{3,j} < e) \wedge (v_3 = 1)\right) \end{array} : \text{Exp}_1^{\mathcal{A}}(\text{input})\right] \leq \mu(\lambda)$$

PAYMENT PROJECT

Authorised Push Payment (APP) Fraud

Our Solution

2. **Efficient Protocol:** we designed an efficient protocol that realises the PwDR's definition.

    - formally proved the protocol is secure (i.e., meets the formal definition).

3. **Analysed the Protocol's Cost:** we performed a cost analysis of the construction via both asymptotic and runtime evaluation (via a prototype implementation).

PAYMENT PROJECT

Protecting Victims of APP Frauds

Main Tools We Used

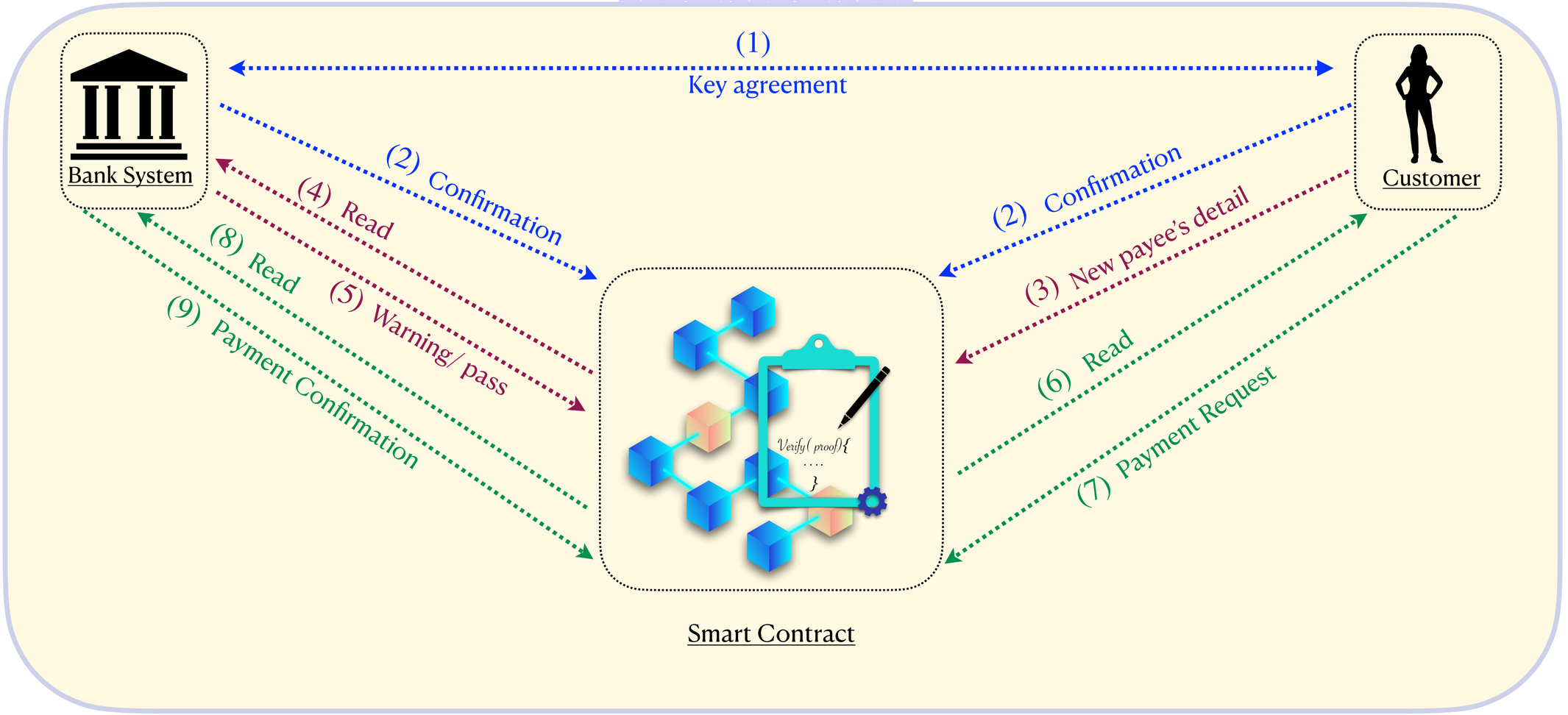
- The PwDR Protocol's building blocks:
  - Commitment scheme
  - Digital signature
  - Smart contract
  - Pseudorandom function
  - Bloom filter
  - Threshold voting protocols

PAYMENT PROJECT

Protecting Victims of APP Frauds

The PwDR Protocol's Workflow

Payment Phase

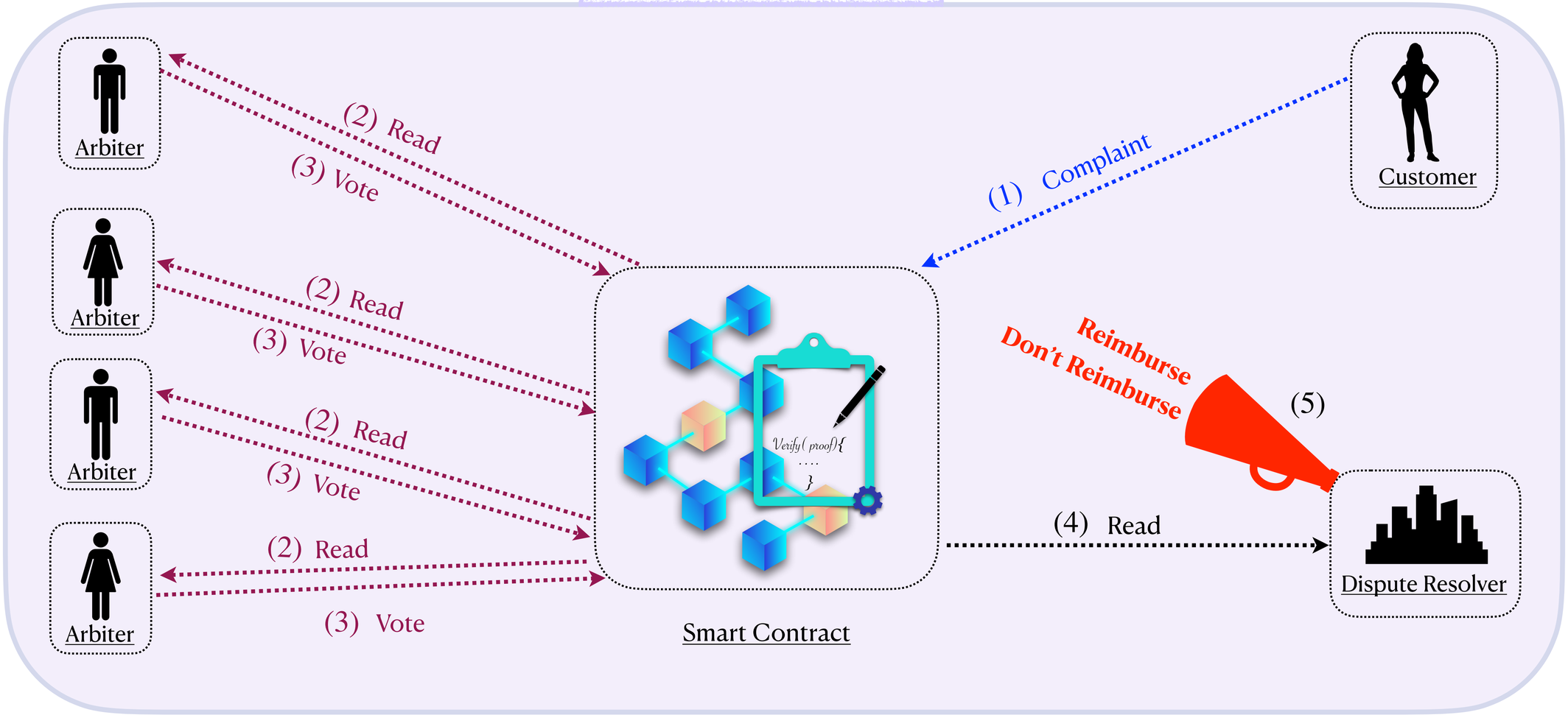


PAYMENT PROJECT

Protecting Victims of APP Frauds

The PwDR Protocol's Workflow

Dispute Resolution



PAYMENT PROJECT

Protecting Victims of APP Frauds

The PwDR Protocol's Complexity

Party	Setting		Computation Cost	Communication Cost
	$e = 1$	$e > 1$		
Customer	✓	✓	$O(1)$	$O(1)$
Bank	✓	✓	$O(1)$	$O(1)$
Arbiter $\mathcal{D}_1, ..., \mathcal{D}_{n-1}$	✓	✓	$O(1)$	$O(1)$
Arbiter $\mathcal{D}_n$	✓		$O(n)$	$O(1)$
		✓	$O(\sum_{i=e}^{n} \frac{n!}{i!(n-i)!})$	$O(\sum_{i=e}^{n} \frac{n!}{i!(n-i)!})$
Dispute resolver	✓	✓	$O(n)$	$O(1)$

n: number of arbiters

e: threshold

PAYMENT PROJECT

Protecting Victims of APP Frauds

The PwDR Protocol's Runtime in Millisecond

Party	$n = 6$		$n = 8$		$n = 10$		$n = 12$	
	$e = 1$	$e = 4$	$e = 1$	$e = 5$	$e = 1$	$e = 6$	$e = 1$	$e = 7$
Arbiter $\mathcal{D}_n$	0.019	0.220	0.033	0.661	0.035	2.87	0.052	10.15 *
Dispute resolver $\mathcal{DR}$	0.001	0.015	0.001	0.016	0.001	0.069	0.003	0.09

n: number of arbiters

e: threshold

PAYMENT PROJECT

Protecting Victims of APP Frauds

Conclusion

- To protect victims of APP frauds, we proposed "Payment with Dispute Resolution" (PwDR) scheme.
- We hope that our result lays the foundation for future solutions that will protect victims of APP frauds.

The end