Analysing, Modelling, and Transforming Online Payment Systems Security

Dr Aydin Abadi

My research vision is to revolutionise online payment systems (i.e., Online Banking and cryptocurrency) to **tackle online fraud at its root**, by (a) **analysing** online payment systems' security: to discover their fundamental weaknesses in dealing with online fraud, (b) **modelling**: to establish scientific foundations for the core security guarantees that an online payment system must offer to resist online fraud, and (c) **transforming**: to devise security protocols that will significantly improve online payment systems' security against online payment fraud. Thus, my research will answer two primary questions: (1) why do online payment systems fail to resist online payment fraud? and (2) how can we develop much stronger online payment systems?

The proposed research programme draws on my unique combination of skills in cryptography, applied mathematics, cryptanalysis, and computer programming developed through collaborating with top-tier scientists, writing over 23 technical publications, and developing over 7 open-source prototypes and software.

1 Context

Online Banking (OB) is an internet-based system that is now popular among people in the UK and around the world. OB has also drawn considerable attention from fraudsters who want to illegally transfer money from a victim's bank account to their bank account; this type of fraud is also known as OB fraud. Only in the first half of 2021, fraudsters stole a total of £464.2 million through OB fraud in the UK, an increase of over 67% compared to the same period in 2020 [1]. Both UK residents and banks have been suffering from this type of fraud. The level of online payment fraud in the UK is such that it is **now a national security threat** [2]. There have been efforts to deal with OB fraud, by using (a) prevention mechanisms, such as 2-Factor Authentication (2-FA) schemes that lower the chance of fraudsters who want to gain unauthorised access to users' OB accounts, or Confirmation of Payee (CoP) that ensure a money recipient details (inserted by the money sender) matches the record held by the recipient's bank and (b) protection mechanisms, that mainly include regulations about how to reimburse victims of fraud. Nevertheless, the increasing amount of money lost to this type of fraud indicates that the current ad-hoc prevention mechanisms are ineffective. The current level of victim protection and reimbursement rate is low too; for example, only 42% of the stolen funds were returned to victims of "Authorised Push Payment" (APP) frauds in the UK, in the first half of 2021.

CryptoCurrency (CC) is another online payment system that has been drawing the attention of individuals and industry, since its introduction in 2009. Fraudsters have been defrauding CC users regularly. For instance, only in 2021, people in the UK and US have reported losing about £146 million and $1 billion in cryptocurrency to fraud respectively [3, 4]. But, for CC there exists no fraud prevention and protection technical mechanisms.

Online fraud is a **global phenomenon**. According to the FBI, only victims of APP fraud reported at least a total of $419 million in losses, in 2020. Although it has been over a decade since the introduction of online payment systems, there exists no scientific approach to *fundamentally* deal with online payment fraud.

2 Critical Limitations of State-of-the-art

Research on enhancing the security of online payment systems is evolving. There have been various efforts to improve fraud detection or prevention mechanisms, e.g., in [5, 6, 7]. Nevertheless, all existing works share similar shortcomings; they focus on very specific types of fraud (e.g., impersonation or Ponzi scheme), take reactive approaches (i.e., they offer solutions that are dependent on fraudsters' known strategies), offer no remedy for protecting victims of fraud, and miss the big picture [8, 9]. Specifically, to date, (1) there exists no rigorous analysis of online payment systems (i.e., OB and CC) to discover the **fundamental security flaws** that make them susceptible to online fraud, (2) there is no mathematical **formal model** that defines the core guarantees that online payment systems must provide to resist online fraud and/or reimburse fraud victims, even if the systems **evolve** (i.e., composed with future technologies), and (3) there is no concrete **provably secure security protocol** (i.e., a set of accurate mathematical procedures) that offers the fundamental security guarantees. Dependability (e.g., security and availability) in the face of system **evolution** itself is a crucial research line and is one of computer science's *grand challenges* in a different context, i.e., "dependable systems evolution" in software engineering [10]. Also, devising formal models is very valuable, not only because it is required as a basis to precisely state security properties and to perform formal analysis, but also because it summarizes vital aspects in several specifications that are otherwise spread across various documents [11].

3 A Novel Scientific Approach

The proposed research will address the above critical limitations by using a novel scientific approach; namely, via analysing, modelling, and then transforming online payment systems' security against online fraud. In this research for the first time, I will consider each class of online payment system (i.e., OB and CC) and its components as a single unit and will conduct a rigorous security analysis to understand why it fails to resist online fraud. This approach differs from the existing ones which only analyse the security of new components, without ensuring they will not introduce new vulnerabilities when they are combined with existing systems.

I will also develop new mathematical models to define the core security guarantees that a protocol must offer to resist online fraud, by using a unique combination of "Universally Composable" (UC) and game theory models. This will (1) let future security protocols based on the model remain secure even if they are combined with other components without affecting the overall security, and (2) capture the real-world settings where adversarial behaviours are motivated by financial incentives. I will also devise (a) a new privacy-preserving real-time risk analysis protocol (for OB) and a new digital wallet (for CC) by relying on Private Set Intersection (PSI) and (b) the first secure fair exchange protocol that will support generic digital services.

I will focus on victim protection mechanisms and develop security protocols that will help victims of online payment fraud receive reimbursement by using a new combination of an "insurance-like" mechanism and a privacy-preserving voting scheme. These mechanisms have the potential to yield new Fintech insurance startups that will provide users of CC with protection against cryptocurrency fraud. Finally, my research will also produce two novel frameworks to incentivise banks to use stronger security defences not only against OB fraud but also against insider threats. The first framework will rely on a combination of economic incentives and verifiable computation and the second framework will use cloud computing security models and privacy-preserving verifiable computation. Neither combination has ever been used before in the context of banking.

4 The Research Programme

4.1 Project Partners and Research Team

The project's partners will include (1) an international company, e.g., "Informatica", "Mysten Labs", or "Lyzis Labs", (2) two internationally leading academics in the field of information security and cryptography, i.e., Prof. Yvo Desmedt from the University of Texas at Dallas and Prof. Changyu Dong, Director of Research at Guangzhou University, and (3) two academics in the field of Human-Computer Interaction or Human Aspects of Security. My research team at UCL will consist of a PhD student (PhD-S) and two Post Doctorate Research Associates (PDRA-1 and PDRA-2).

The research project requires (a) developing mathematical models, (b) devising cryptographic protocols and (c) implementing protocols. I will recruit two researchers, each of whom will work for two years on this project. I will ensure they will have adequate experience. PDRA-1 will develop security models, design cryptographic protocols and implement the protocols (for OB and CC), while PDRA-2 will develop security models and devise cryptographic protocols (for OB).

4.2 The Research Objectives and Methods

The research will have the following six broad objectives.

- Objective 1 (O-1): Discovering Fundamental Security Flaws of Online Payment Systems.
- Objective 2 (O-2): Developing New Mathematical Security Models.
- Objective 3 (O-3): Transforming Online Payment Systems Security Defences.
- Objective 4 (O-4): Transforming Online Payment Systems Victim Reimbursement Mechanisms.
- Objective 5 (O-5): Developing Framework Incentivising Banks to Use Stronger defences.
- Objective 6 (O-6): Developing Framework Making OB Resilient Against Insider Threats.

To achieve the objectives, I envisage a research plan made of six Work Packages (WPs) across five years. Figure 1 outlines my research programme.

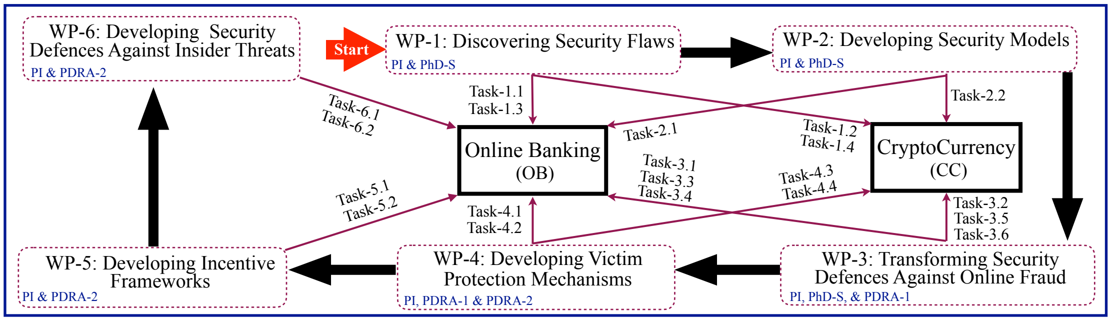

Fig. 1: The Research Programme Outline

WP-1: Discovering Fundamental Security Flaws of Online Payment Systems– O-1 (Month 1–12)

I will identify the fundamental weaknesses of the existing payment systems' security protocols in dealing with online fraud, when each protocol works in *isolation* and when it is *combined* with other security mechanisms.

• **Methodology:** In this WP, I will leverage my cryptanalysis skills, i.e., my previous experience in discovering major security flaws in various security protocols that were thought to be secure and published in top-tier venues, e.g., see [12, 13, 14]). To identify the systems' security flaws, first I will conduct **data collection** for OB (Task-1.1) and CC (Task-1.2), by collecting the following three sources of data from the literature: (i) existing security protocols and their initial security requirements, (ii) fraudsters' strategies, and (iii) victims' behaviour that made them fall victims to the fraud. Then, I will conduct **data processing**, for OB (Task-1.3) and CC (Task-1.4) via (a) analysing the security protocols to discover the core flaws that made the protocols unable to capture the security requirements, fraudsters' strategies, and victims' behaviour, and (b) analysing the protocols' initial security requirements to discover mismatches between these requirements, fraudsters' strategies, and victims' behaviour. The security analysis conducted in this WP will be **manual**. It will involve **cryptanalysis** of each OB and CC and its subprotocols as a single unit. The reason for using manual cryptanalysis is that there exists no automated verification mechanism that can precisely identify systems' security flaws that make them susceptible to online payment fraud. PhD-S will assist me in this WP.

• **Outcome:** A list of weaknesses of current OB and CC that make them susceptible to online payment fraud.

• **Novelty:** The first research that will consider a combination of an online payment system and its components as a **unit** and conduct a **security analysis of the unit** to understand **why it fails to resist online fraud**.

WP-2: Developing New Mathematical Security Models– O-2 (Month 7–20)

In general, to design a provably secure security protocol, it is vital to first formally define the protocol's central security requirements. However, existing OB and CC lack such definitions when it comes to online fraud. Currently, when a certain type of fraud becomes popular, security experts propose ad-hoc patches to deal with that specific fraud, without formally analysing whether the proposed patch would work and/or would not impose new security risks on the existing protocol. In this WP, **for the first time**, I will develop a mathematical security model, to set accurate scientific foundations for the core security guarantees that a protocol must offer to resist online fraud. The model will consider the findings in WP-1.

- **Methodology:** In Task-2.1 and Task-2.2 I will develop mathematical security models for OB and CC respectively. I will establish each security model based on a **unique combination** of a strong formal cryptographic model (i.e., simulation-based "Universally Composable" (UC) paradigm) and game theory. The use of the Universally Composable paradigm will ensure that any protocols that will be based on the proposed model will remain secure even if multiple instances of the protocols (a) are executed in parallel, which often occurs in the real world when multiple users invoke the same protocol at the same time, or (b) are composed with other protocols, which will allow new future inventions/technologies to be integrated into to the existing ones without affecting the overall security (according to the composition theorem [15]). In general, standard security/cryptographic models (such as UC) ensure that any protocol that realises them would remain secure regardless of adversaries' strategies. The use of game theory will ensure that the proposed model will capture the real-world settings in which adversarial and fraudulent behaviours are motivated by financial incentives. Thus, the models that I will propose in this WP will ensure that even a highly intelligent fraudster, that may benefit from **Artificial Intelligence**, cannot violate the security guarantees of any security protocol that realises them. My previous research that involved developing various simulation-based models (e.g., see [14, 16, 17, 20, 28, 29]) will be a helpful foundation for this WP. I will also improve my knowledge of UC and game theory during the research. PhD-S will help me in this WP.
- **Outcome:** Formal security models for OB and CC.
- **Novelty:** The first research that will develop a **security model which considers online payment fraud** for each class of online payment systems by using a unique **combination of UC** and **game theory** models.

WP-3: Transforming Online Payment Systems Security Defences– O-3 (Month 15–39)

In WP-3, I will transform OB's and CC's security by building much stronger provably secure security protocols.

- **Methodology:** In this WP, I will leverage my previous research in CC, experience in using (and teaching) C++ , Solidity, as well as developing PSI protocols (e.g., in [12, 14, 17, 20, 26]), smart contracts (e.g., in [13, 18, 19, 26]), authentication schemes (e.g., in [27]), and fair exchange protocols (e.g., in [13, 18]).

I will analyse the existing security protocols designed to combat online fraud in OB (Task-3.1) and CC (Task-3.2). In the same tasks, I will improve them, so they can fit the models. To further improve security, I will develop new security protocols. Specifically, in Task-3.3, I will develop **new effective tools** that will let each bank **identify suspicious accounts and transactions** through user profiling, strong authentication mechanisms, and privacy-preserving identity management systems that require account holder users to provide more information (than what they currently do) to justify each transaction while preserving users' privacy. PhD-S and PDRA-1 will assist me in Task-3.1–Task-3.3.

In Task-3.4, I will design **the first security protocol** that will perform **real-time risk analysis** via performing **privacy-preserving data sharing nationwide**, among different banks and the government. The result of the analysis will be given to a payer and payee before they complete a transaction. Thus, the protocol will check multiple private databases, including all (UK) financial institutions' databases of blacklisted customers, and the government's databases of blacklisted individuals, e.g., in [25]. To build the risk analysis protocol, I will use a (threshold) PSI as a subroutine. PSI is a cryptographic protocol which allows parties to find the intersection of their private sets, without being able to learn anything beyond the result.

This risk analysis protocol will be invoked by the payer's bank, say $\mathcal{B}$, when the payer wants to transfer money. The input of each database holder, except $\mathcal{B}$, to the PSI, will be the payer's ID concatenated with a binary flag F associated with the ID, i.e., $ID||F$. Note, $F = 1$ if the database holder considers the customer suspicious and $F = 0$ otherwise. $\mathcal{B}$'s input to the PSI is $ID||1$. After the PSI's execution, $\mathcal{B}$ receives only $ID||1$ from the PSI if a certain number of database holders have identified the same customer as suspicious; otherwise, it receives nothing. The use of PSI will ensure that a bank will only learn whether a certain customer was flagged as suspicious by its counterparties. I will implement the protocol and analyse its runtime.

In Task-3.5, I will design **the first protocol that can perform real-time risk analysis in CC** via (i) creating a database of blacklisted CC users and (ii) designing a digital wallet that will perform risk analysis (and inform users) using the database. The database in this phase will be maintained decentrally (e.g., by a smart contract), where the entries of this database are (a) blacklisted banks customers and individuals whose details are inserted into the database by banks and governments and (b) blacklisted CC users, whose details are inserted into the database by an authorised committee of auditors that verify and vote whether a nominated user's detail must be inserted into it. To enhance privacy, the database will be encrypted. To transfer digital money, users can use the new digital wallet devised in Task-3.5. In this case, when the user wants to transfer digital money to a payee, the wallet will perform a risk analysis, in a privacy-preserving way, and checks if the payee's details are not in the database. It will inform the user about the analysis result. To achieve privacy, I will use PSI which will allow the wallet to read only an element of the database without revealing: (a) to the smart contract (holding the database) which element was read and (b) to the wallet other elements of the database. I will use the PSI that I designed in [20] to develop the risk analysis protocol. This PSI is highly suitable as it is efficient and lets only one of the parties (e.g., the wallet) learn the result; thus, the smart contract cannot learn which element the result recipient reads from its database. Also, this PSI enables the smart contract to make sure that at most a single element of its database will be read by the wallet. Because, in this PSI, each party represents its set $S = \{e_1, ..., e_n\}$ as a polynomial: $P(x) = \sum_{i=1}^{n}(x - e_i)$ and sends the (encrypted) polynomial to its counter-party. Given the (encrypted) polynomial, the smart contract can check if its degree is one to ensure it represents only a single value.

Task-3.6 will focus on fair exchange protocols, which are useful mechanisms to reduce the rate of online fraud occurrence (in CC), as they allow a payer to pay if and only if it receives the digital items/services it wants to pay for. However, as I have previously shown (in [18]), the only fair exchange protocol that supports digital services suffers from serious security issues. In Task-3.6, I will design a new **generic fair exchange protocol** for a **wide class of digital services**, e.g., any verifiable computation. It will prevent a broad class of fraud in CC, e.g., it will deal with any fraudsters that pretend to be legitimate online service providers, but would not deliver promised services as soon as they are paid by clients for the services. To design the protocols, I will use non-interactive Zero-Knowledge proofs and smart contracts. I will implement this protocol and analyse its computation cost. My initial study, presented in the 55-page technical paper in [18] has demonstrated the feasibility of designing secure generic fair exchange protocols. Note that all protocols, that I will design in different WPs, will be accompanied by formal security proofs asserting that the protocols satisfy the requirements of the models developed in WP-2. PhD-S will assist me in Task-3.4–Task-3.6.

- **Outcome:** (a) risk analysis protocols for OB and CC, (b) a generic fair exchange protocol for CC, (c) two open source packages that implement the risk analysis protocol for OB and the fair exchange protocol, and (d) new tools that will let each bank identify suspicious accounts/transactions.
- **Novelty:** the **first**: (1) systematic analysis of online payment system which will identify existing **non-composable** protocols, (2) real-time risk analysis protocol that will use **privacy-preserving** data sharing techniques, (3) **digital wallet that will perform privacy-preserving risk** analysis **through PSI**, and (4) secure fair exchange protocol that will support **generic** digital services.

WP-4: Transforming Online Payment Systems Victim Protection Mechanisms– O-4 (Month 30–42)

It would be unrealistic to assume that any payment security protocol will remain secure against online payment fraud all the time (as human errors can benefit fraudsters). In this WP, I will significantly improve the **reimbursement** level of fraud victims in OB and CC, in the case where fraudsters succeed.

- **Methodology:** I will leverage my previous research in CC (e.g., see [16]) and experience in designing a protocol (in [21]) that can help fraud victims receive compensation, to complete the tasks in this WP. In Task-4.1, I will **develop a mathematical** model to set the core security guarantees that OB must offer **to reimburse honest victims of online payment fraud**. The model will formalise the existing regulations, e.g., the "Contingent Reimbursement Model" (CRM) code that protects customers. The model will use a cryptographic model and will offer three crucial properties: (i) security against a malicious victim, (ii) security against a malicious bank, and (iii) privacy. PDRA-1 will assist me in Task-4.1.

In Task-4.2, I will **develop a protocol** to help fraud victims be reimbursed. The protocol will need to (1) enable honest victims to generate proof proving their innocence, (2) rely on tamper-evident privacy-preserving transaction logs, (3) enable a committee of neutral auditors to verify and vote on the validity of victims' proof, and (4) preserve the committee members' verdicts. The protocol will use (a public) blockchain to log the transactions between the customer and the bank. It will also involve (a) a committee of auditors that compile customers' complaints and provide their (encoded) verdicts, and (b) a dispute resolver which aggregates the auditors' votes and announces the final verdict. At a high level, the protocol will work as follows.

Initially, a customer and bank agree on a Smart Contract ($\mathcal{SC}$). They also agree on a secret key. Then, the customer and bank use a commitment scheme to commit to the secret key. Each of them sends the resulting commitment to $\mathcal{SC}$. When the customer wants to transfer money to a new payee, it signs into its OB account. It generates an update request (that specifies the new payee's detail), encrypts it (using the key), and sends the result to $\mathcal{SC}$. Then, the bank decrypts and checks the request, e.g., to determine whether it meets its internal policy. Depending on the request, the bank generates a pass or warning message. It encrypts the message and sends the result to $\mathcal{SC}$. The customer checks the bank's message and decides whether to make a payment. If it decides to do so, it sends an encrypted payment detail to $\mathcal{SC}$. The bank decrypts the message, locally transfers the specified amount of money, and sends an encrypted "paid" message to $\mathcal{SC}$.

Later, when the customer realises that it has fallen victim, it raises a dispute by generating an encrypted complaint that can challenge the effectiveness of the warning and/or any payment inconsistency. It encrypts the complaint and sends to $\mathcal{SC}$ the result and the proof asserting the secret key's correctness. Each auditor verifies the proof. If the verification passes, the auditor decrypts and compiles the customer's complaint to generate a verdict. Each auditor encodes its verdict (using an e-voting mechanism that I designed in [21]) and sends the encoded verdict's encryption to $\mathcal{SC}$. To resolve a dispute, either the customer or bank directly sends to the dispute resolver the secret key and proof asserting that the key was generated correctly. The dispute resolver verifies the proof. If approved, it locally decrypts the encrypted verdicts and learns the final verdict. If the final verdict indicates the legitimacy of the customer's complaint, then the customer must be reimbursed. My initial study, presented in a 31-page technical paper in [21], shows the feasibility of achieving the above objective. PDRA-1 and PDRA-2 will assist me in Task-4.2.

In Task-4.3, I will **develop a mathematical model** that captures the main requirements that CC must satisfy to reimburse victims of online payment fraud. It will use a **novel combination** of (i) the models and theories used in the **insurance industry** (e.g., Poisson process and ruin theory) and (ii) the simulation-based UC paradigm, to ensure that any solutions fitting this model can compensate fraud victims and can be securely composed with CC. In Task-4.4, I will **devise a security protocol** that matches the model; it will use a combination of Ethereum smart contracts, a deposit paradigm, and e-voting schemes. It will involve five types of parties: (a) servers, each of which is a service provider which accepts cryptocurrency in exchange for the service it provides (e.g., investments in cryptocurrency), (b) clients, each of which is a customer of a server, (c) a standard smart contract ($\mathcal{SC}$), (d) a committee of auditors, consisting of trusted third-party auditors that compile complaints and provide their verdicts, and (e) an insurance operator ($\mathcal{O}$), a third party whose main role is to register the (address of) servers and auditors into the smart contract $\mathcal{SC}$.

At a high level, the protocol will work as follow. First, $\mathcal{O}$ deploys a Smart Contract ($\mathcal{SC}$). Then, $\mathcal{O}$ registers a set of servers and auditors. After that, financial interactions between a client and a registered server are performed via $\mathcal{SC}$ which charges them a **premium**. Later, when a client realises it has been defrauded by a registered server, it raises a dispute, by sending a complaint message to $\mathcal{SC}$. The client can include in the complaint pieces of evidence too. Each auditor compiles the complaint and sends its verdicts to $\mathcal{SC}$ which comes to the final decision based on all auditors' verdicts. If $\mathcal{SC}$ concludes that the client must be reimbursed, then $\mathcal{SC}$ reimburses the client. PDRA-2 will assist me in Task-4.3 and Task-4.4.

- **Outcome:** Two mathematical models (for OB and CC) and two security protocols that can help victims of OB and CC fraud receive compensation for their financial losses to fraud.
- **Novelty:** The **first**: (1) protocol that will **use current regulations** and help **OB fraud victims receive reimbursements** and (2) **insurance** that will help **cryptocurrency fraud victims receive compensation**.

WP-5: Developing Framework Incentivising Banks to Use Stronger Defences– O-5 (Month 42–51)

- **Methodology:** In this WP, I will leverage my experience in developing incentive frameworks (e.g., in [22, 23]), to develop a formal framework that **incentivises banks** to implement stronger security defence against online payment fraud. In Task-5.1, I will develop a mathematical model **informed by the real-world economic incentives** that motivates banks to use stronger security protocols to deal with online payment fraud. The model will ensure that there will be a **negative correlation** between (1) the bank's online fraud occurrence rate and (2) its reputation and revenue. It will also capture the notion of undeniability to ensure that banks cannot deny frauds that occur on their OB. The model will rely on a combination of economics and a formal cryptographic model. In Task-5.2, I will also develop a provably secure framework (i.e., a generic security protocol) that can fit into the model. It will enable fraud victims to report fraud occurrences to an authorised committee which verifies whether the bank is liable for that. The verification outcome is stored in a public secure repository. The framework will let various functions run on the above verification outcomes, e.g., to determine a bank's current reputation/ranking. The functions' outputs can be publicly verified. The framework will ensure that the above functions' outcomes are taken into account in critical trades between the bank, its customers, its business partners, or the government. To construct the framework, I will use tamper-proof logs, verifiable computation, and digital signatures. PDRA-2 will help me in this WP.

• **Outcome:** (a) a security model that defines factors and security requirements needed to make banks use stronger security protocols to deal with online fraud, and (b) a security framework realising the model.

• **Novelty:** This will be the first research developing a **model and framework** using a **unique combination of economic factors** and **verifiable computation** to incentivise banks to employ stronger security defences.

WP-6: Developing Framework Making OB Resilient Against Insider Threats– O-6 (Month 50–60)

Insider attacks are imminent threats to banks and their customers. Insiders may collude with external fraudsters. The data that insiders can gather about their customers is very valuable. Tempering with customers' data and the computation executed on them will have serious repercussions for banks and their customers. Although there have been ad-hoc proposals (e.g., penetrating testing) to address the issue, the effectiveness of the proposals has never been scientifically proven. Also, they cannot provide assurance to customers that the critical computations on their data (e.g., to create account statements) were conducted correctly.

• **Methodology:** In this WP, I will take a **new approach** to address the issue. I will rely on my experience in developing models and protocols that guarantee security against insider threats in cloud computing (e.g., in [17, 24, 26]) to attain this WP's objective. In Task-6.1, I will develop a new mathematical security model using **paradigms developed for "cloud computing"**. Cloud computing security models assume the cloud is not trusted and is susceptible to insider (and outsider) attacks. Also, in Task-6.2, I will devise a framework that satisfies the model's security requirements. The framework will enable customers (machines) to locally compile their sensitive data, which would yield encoded data and metadata that can be stored on the banks' servers. The data stored on the bank's servers will not leak any information about the customer's original sensitive data. The platform will also enable customers to verify any computation executed on their encoded data, with the assistance of the metadata. I will build the platform by using homomorphic encryption and privacy-preserving verifiable computation. PDRA-2 will help me in this WP.

• **Outcome:** A formal security model that defines the security requirements to deal with insider threats in banks and a security framework that realises the model.

• **Novelty:** The first research that will develop a **security model** and **framework** using a **cloud computing security models** and **privacy-preserving verifiable computation** to deal with insider threats in banks.

5 National Importance and Impacts

Academic Importance and Impact. My proposed research will benefit both OB and CC research communities. The discovered weaknesses (in WP-1) will be valuable criteria for software engineers and security experts when designing a payment system. The mathematical models (in WP-2 and WP-4) will serve as a solid basis for the systematic evaluation of existing/future payment systems' security and victim protection levels. The security protocols (in WP-3 and WP-4) will enable researchers to understand what techniques and computational hardness assumptions must be relied upon to build a secure online payment system. This research (in WP-5 and WP-6) will benefit other sectors' researchers (e.g., in the healthcare or airline) that seek to incentive those sectors to implement stronger security defences and protect themselves from insider threats.

To ensure my research will have a maximum academic impact, I will: (a) **publish and present research findings** at conferences, and (b) **maintain an online anti-fraud database** on the project's website.
Societal Importance and Impact. The result of this research can benefit UK residents from financial and mental health perspectives, by helping lower the amount of money lost to fraud and protecting victims of fraud. To share the findings with the public, I will (1) **maintain public-facing communication channels**, via creating social media posts, (2) **deliver webinars at schools and universities**, to inform young people about online payment fraud, and (3) **engage with the public in science festivals**.
Economic Importance and Impact. This research will benefit UK banks, by revolutionising their online payment systems. Hence, they will lose far less to fraud. I expect this research (i.e., WP-4) to result in **new Fintech insurance startups** that will provide users of CC with protection against cryptocurrency fraud. This has the potential to make the UK a base for international investment in this *new line of the insurance industry*. To maximise the research's economic impacts, I will (1) **share the research findings with UK regulators**, as I have done in the past via inviting them to seminars and having regular meetings with them (2) **meet with UCL Public Engagement** to seek effective ways to draw investors' attention to the research findings.

6 Risks and Mitigations

I will use a combination of **traditional** and **Agile methodology** for risk management which will allow me to identify potential risks and mitigations before the onset of the project and throughout the project lifecycle. So far, I have identified a set of technical and non-technical risks and related mitigations. In WP-1, there is a risk that the literature and my research's findings capture very few strategies of fraudsters. To mitigate it, I will cross-check the findings of the research with consumer protection organisations and will consider their input; more importantly, I will ensure that the security models, that I will propose in the next WPs, will be independent of adversaries' strategies. In WP-3, it is possible that a direct combination of existing tools and techniques would not satisfy the models' requirements; in this case, I will adjust the underlying building blocks to ensure they will meet the requirements while ensuring that adjustments will not affect their original security guarantees. In WP-4, there is a risk that the protocol that I will develop would impose high costs that could negate its benefits. In this case, I will improve the protocol's efficiency by relying on data structures, such as the Merkle tree. It is possible that some of the project partners will stop their collaboration with the research project. In this case, I will find replacement partners, e.g., Prof. Aggelos Kiayias or IOHK company.

7 Development Plan

To attain my goals, during the research program, I will (1) **join UCL's Research Staff Development Programme**: this will allow me to improve and develop the necessary skills to successfully lead a research team and a lab, (2) **improve my knowledge of Responsible Research and Innovation**: to ensure my research follows the principles of responsible innovation (i.e., anticipate, reflect, engage, and act) I will (i) consult with the UCL ethics community, social scientists in UCL, and the academic members of (the project partner) in every WP of the research project and (ii) take the online "Responsible Innovation course" provided by UCL, (3) **give talks** at national and international seminars and conferences (e.g., FC), (4) **join training courses for "Universal Composability" (UC) and Game theory**: I will join the training courses provided by Ran Canetti (the inventor of UC) and UCL Department of Economics, respectively, and (5) **expand my network and collaboration**, e.g., by hosting international workshops.

References. **[1]** UK Finance, "2021 half year fraud update", 2021. **[2]** UK Finance, "Government-coordinated action needed as fraud losses rise by 30 per cent", 2022. **[3]** National Fraud and Cyber Crime Reporting Centre, "Cryptocurrency fraud leads to millions in losses so far this year", 2021. **[4]** Federal Trade Commission, "Reports show scammers cashing in on crypto craze", 2022. **[5]** H. H. AL-Abri, B. Kumar, and J. Mani, "Improving fraud detection mechanism in financial banking sectors using data mining techniques", 2021. **[6]** S.

M. S. Askari and M. A. Hussain, “Intuitionistic fuzzy logic based decision tree for e-transactional fraud detection”, 2020. **[7]** E. Jung, M. Le Tilly, A. Gehani, and Y. Ge, “Data mining-based Ethereum fraud detection”, 2019. **[8]** O. Syniavska, N. Dekhtyar, O. Deyneka, T. Zhukova, and O. Syniavska, “Modelling the process of counteracting e-banking fraud”, 2019. **[9]** M. Carminati, M. Polino, A. Continella, A. Lanzi, F. Maggi, and S. Zanero, “Security evaluation of a banking fraud analysis system”, 2018. **[10]** T. Hoare and R. Milner, “Grand challenges for computing research”, 2005. **[11]** D. Fett, R. Kusters, and G. Schmitz, “An expressive model for the web infrastructure”, 2014. **[12]** A. Abadi, S. J. Murdoch, and T. Zacharias, “Polynomial representation is tricky: Maliciously secure private set intersection revisited”, 2021. **[13]** A. Abadi, S. J. Murdoch, and T. Zacharias, “Recurring contingent payment for proofs of retrievability”, 2021. **[14]** A. Abadi, S. Terzis, and C. Dong, “Delegated private set intersection on outsourced datasets”, 2015. **[15]** R. Canetti, “Universally composable security: A new paradigm for cryptographic protocols”, 2001. **[16]** A. Abadi, M. Ciampi, A. Kiayias, and V. Zikas, “Timed signatures and zero-knowledge proofs: time-stamping in the blockchain era”, 2020. **[17]** A. Abadi, C. Dong, S. J. Murdoch, and S. Terzis, “Multi-party updatable delegated private set intersection”, 2022. **[18]** A. Abadi, S. J. Murdoch, and T. Zacharias, “Recurring contingent service payment”, 2022. **[19]** A. Abadi, “Aydin Abadi’s GitHub repository”, https://github.com/AydinAbadi?tab=repositories. **[20]** A. Abadi, S. Terzis, R. Metere, and C. Dong, “Efficient delegated private set intersection on outsourced private datasets”, 2019. **[21]** A. Abadi and S. J. Murdoch, “Payment with dispute resolution: A protocol for reimbursing fraud victims”, 2022. **[22]** A. Abadi, L. Trotter, M. Harding, P. Shaw, N. Davies, C. Elsden, C. Speed, J. Vines, and J. Hallwright, “Smart donations: Event-driven conditional donations using smart contracts on the blockchain”, 2020. **[23]** A. Abadi, J. Xiao, R. Metere, and R. Shillcock, “ValuED: A blockchain-based trading platform to encourage student engagement in higher education”, 2021. **[24]** A. Abadi, “Delegated private set intersection on outsourced private datasets”, 2017. **[25]** The Insolvency Service, “Director disqualification outcomes”, 2022. **[26]** A. Abadi, and A. Kiayias, “Multi-instance Publicly Verifiable Time-Lock Puzzle and Its Applications”, 2021. **[27]** A. Abadi, and S. Murdoch, “A Forward-secure Efficient Two-factor Authentication Protocol”, 2022. **[28]** L. Martinico, A. Abadi, and T. Zacharias, T. Win, “A Generic Transparent Privacy-preserving Exposure Notification Analytics Platform”, 2022. **[29]** A. Abadi, S. Terzis, and C. Dong, “VD-PSI: Verifiable Delegated Private Set Intersection on Outsourced Private Datasets”, 2016.