Abstract

The aim of this project is to investigate off-chain protocols (or so-called layer 2) as a scaling solution for the cryptocurrencies (and distributed ledger technologies in general). Intuitively, an off-chain protocol let a group of parties execute the terms of a smart contract locally amongst themselves with the same security guarantees of the global distributed ledger network. With our partners null and the null, we'll focus on resolving outstanding research problems that hinder off-chain protocols from real-world use. This supports the digital economy initative as it will support the UK's understanding of how blockchain technology and smart contracts can impact our financial economy.

1 Introduction

Since the emergence of Bitcoin in 2009, we have witnessed the rise of blockchains. Bitcoin proposed the first global public ledger that enacts the *trust, but verify* paradigm. The only trust in Bitcoin is that at least 51% of the network's miners include recent transactions in the public ledger. Other than that, anyone can independently verify the validity of all financial transactions on the network. The unprecedented transparency and security demonstrated by Bitcoin has led to an entire new market for the financial economy which peaked with a market capitalisation of over $1tn in January 2018. Furthermore, some prominent followers such as Ethereum, Difinity and Cardano are taking the innovation underpinning Bitcoin further by supporting the storage and execution of smart contracts as opposed to only financial transactions.

Smart contracts aim to replace human-operated services with verifiable and programmatic intermediaries by allowing anyone to verify the contract's execution. Its destructive potential have been acknowledged. Companies (including FTSE 100) are exploring how smart contracts can enable new and global use-cases such as decentralised management for self-sovereign identities, decentralised and non-custodial currency exchanges, supply chain management, etc. Nasdaq have recently published how they are moving beyond a proof of concept usage for smart contracts (and the blockchain), and Fidelity Investments who manage over $5.1 trillion assets on behalf of 10,000 institutional investors have recently launched digital assets which is a cryptocurrency custodial service.

While distributed ledgers with smart contracts can perform frictionless transactions to self-enforce the terms of an agreement, they do not scale. Bitcoin, Ethereum and others only support roughly 10 transactions per second. When this transaction throughput is reached, the network's fee spikes from $0.02 up to $20+ per transaction which is unaffordable for most users. At first glance, it appears that by simply increasing the network's throughput, the scaling issue will be resolved. However, if the network's throughput achieves a significant increase in the realm of 5k transactions per second, it will undermine the 'trust, but verify' principle as honest parties with less resources will no longer be able to independently verify the ledgers correctness (alongside losing the ability to independently validate the execution of smart contracts that interest them). In the worst case, only a handful of wealthy verifiers will have the necessary computational resources to check the ledger's correctness which is essentially the trust assumption that cryptocurrencies were initially designed to replace.

Thus scaling in the context of blockchains is not just increasing the network's throughput, but *increasing the network's throughput without introducing the computational, storage or bandwidth overhead that undermines the 'trust, but verify' paradigm*. This has motivated our track record on designing off-chain (or so-called Layer 2) protocols as an alternative scaling solution for cryptocurrencies (and distributed ledgers in general). In a nutshell, off-chain scaling lets parties transact and execute smart contracts without interacting with the global distributed ledger network while still retaining the same security guarantees. It reduces the network's load as the majority of transactions are processed locally amongst the relevant parties, and the the global distributed ledger network only needs to resolve disputed transactions. So far, state channels and non-custodial sidechains are the two main off-chain scaling proposals which match the same security guarantees as the global distributed ledger network.

The KCL co-PI's research demonstrates several outstanding problems before off-chain protocols can reliably be deployed for real-world use. For example, how can we build an off-chain and non-custodial blockchain with smart contract capability that can compete with a centralised system like Visa's payment network? How can we ensure the incentives are correctly aligned to induce cooperation amongst all parties in the off-chain protocol? How can we assert the non-custodial property such that if the off-chain protocol breaks down then every party gets the coins they deserve? How can we aid the application developer community to pursue a different development paradigm in terms of software and educational tools? We aim the answer the above questions by combining our research strength with the null expertise of our partners the null, null, null, and null.

Novelity and Timeliness Our research provides the cornerstone to scale blockchains to support the following applications (and enterprise use-cases):

- *Enterprise Blockchain:* There has been a surge of interest in blockchain technology from enterprise organisations, including the recently formed Ethereum Enterprise Alliance consisting of 500 firms including JP Morgan, Deutsche Bank, etc. So far, most large enterprises do not perceive public blockchains (like Ethereum) as a suitable platform for business. Public blockchains do not scale, and the risk-appetite of enterprise users does not permit them to use a blockchain that is not operated by a publicly known and reputable maintainer. Our research aims to challenge this perception as off-chain scaling can alleviate both problems. It lets enterprise users execute a smart contract locally amongst themselves, and the global network is only involved if trust amongst the enterprise users breaks down. Furthermore, it lets a reputable and non-custodial operator maintain a distinct blockchain secured by the global blockchain. This lets enterprise users transact on a reputably maintained blockchain with tokens that have real-world intrinsic value.
- *Private Smart Contract Execution:* Off-chain means that if every party co-operates, then a smart contract (and its execution) can remain completely private with the same security guarantees of the global blockchain. In terms of applications, this approach lets parties run smart contracts in a decentralised and private manner. For example, it'll support private auctions without auctioneers, boardroom voting without tallying authorities, casino games without brokers and exchange currencies without match-makers. Furthermore, while the execution can remain private, it also involves no transaction fees as there is no operator to reward and the transaction throughput is only restricted by the local network latency between the co-operative parties.

2 Background

In this section, we'll provide background information about the blockchain, smart contracts, and the state-of-the-art scaling solutions.

Blockchain [1] At a high level, a blockchain is an append-only database that is responsible for ordering transactions. Each block is simply a list of transactions with a pointer to the previous block. The blockchain is designed to be widely replicated and permit any peer to re-execute every transaction to validate its correctness. In other words, every new block performs a batch update on the network and all peers will replicate the update for their local copy of the database.

Nakamoto Consensus [12] The network consists of maintainers and verifiers. The maintainers (i.e. miners who solve a proof of work) are responsible for collecting transactions and appending blocks to the blockchain. The verifiers (i.e. users of the network) are responsible for re-executing every transaction and validating the public ledger's correctness. In other words, the verifiers hold the maintainers accountable and will reject newly minted blocks if it includes invalid transactions. In Bitcoin (and other cryptocurrencies like Ethereum), the maintainers (i.e. miners) compete via a proof of work protocol and each round's winner is eligible to append a new block to the blockchain.

Smart Contract [15] A smart contract is essentially a computer program that is stored, instantiated and executed on the blockchain. Conceptually, it is a trusted third party with public state and it lets parties execute a single program on a global stage without the need to trust each other. Code execution is triggered by transactions accepted into the blockchain. All parties on the network (i.e. verifiers) validate the smart contract's execution by re-executing every transaction and this global replication is the cornerstone for its *self-enforcement property*. The most well-known smart contract platform is Ethereum [16] which supports turing-complete smart contracts.

3 Scalability Solutions

Blockchains do not scale due to the requirement for replicating everything and verifying everything. Currently, there are three general approaches for scaling bockchains:

- New Blockchains: Changing the underyling blockchain into a directed acylic graph [11] or adopting a new consensus protocol [13] can strictly increase the network's throughput.
- Sharding: Partition the peers in the consensus protocol into disjoint shards, and each shard is responsible for processing and verifying some subset of transactions [9].
- Off-chain: A group of parties can process the majority of transactions amongst themselves and the blockchain is only used as a trusted backstop [**?**].

New blockchain protocols and sharding have two major shortcomings: 1) They are not backward compatible and require major changes that must be globally accepted by the network 2) They do not truly solve the scalability dilemma as by strictly increasing the network's throughput, they also reduce the diversity

of verifiers who can hold the maintainers accountable. Furthermore sharding has an additional major shortcoming as each shard only contains a subset of the maintainers, and therefore security is weakened as it becomes easier for an adversary (or a collusion of adversaries) to control the majority of peers in a shard. Without an honest-majority, there is no fail-safe option or mechanism to ensure liveness or integrity of the shard. Our track record has focused on off-chain scaling as by its very nature they avoid the above issues and they are compatible with existing cryptocurrencies (and public blockchains). In the following, we'll focus on the two main off-chain scaling proposals, state channels and non-custodial sidechains.

State Channels. Briefly, a state channel lets a group of n parties execute arbitrary smart contracts amongst themselves. Each party is responsible for verifying the execution of every transaction before digitally signing their agreement to it. State channels are a potential scaling solution as there are no transaction fees for the off-chain transactions, the execution is considered complete after all parties have exchanged a digital signature for it, and each party is protected against a full collusion of all other parties. In terms of track record, the KCL co-PI was among the first with Sprites [**?**] (followed by PISA [**?**] and Kitsune) to design state channels for n parties and to evaluate their applicability for real-world use in the form of a case study.

Sidechain. It create a new blockchain that is maintained by a central operator (or a distributed set of operators). The sidechain is linked to a global blockchain by a two-way peg. The user can enter the sidechain by locking their asset on the global chain and the user always return their final balance back whenever they leave the sidechain. The operator is responsible for digitally signing the order of all transactions, and sending summaries of transactions periodically to the global blockchain. The concept first emerged in Bitcoin for *custodial sidechains* (e.g RSK [10] and Liquid [2]) in which all users must trust the central operator for availability, otherwise they will lose their coins. Recently, Plasma [14] and NOCUST [8] proposed *non-custodial sidechains*. Non-custodial means a dishonest operator cannot confiscate an honest user's coins. A sidechain is more resilient than a state channel as only the operator (and not a single user) can disrupt financial transactions or the execution of smart contracts. However a sidechain still requires fees as the central operator must be rewarded for maintaining the sidechain. In terms of track record, the KCL co-PI performed two in-depth security audits for RSK in 2017-18.

4 Research Challenges for Off-chain and Non-custodial Smart Contracts

There are several fundamental challenges for off-chain solutions before they are ready for real-world use. State channels and sidechains introduce a new security requirement, the **always online assumption**, as all parties must remain online to watch for spurious disputes that publish an earlier state (i.e. a disputer's previous balance). If an honest party is offline for an extended period of time, then they are at risk of losing all their coins. While the KCL co-PI has proposed PISA, an accountable third party watching service for state channels, to help alleviate the always online assumption, it still remains largely an open problem. **How to induce cooperative behaviour** among the transacting parties is another fundamental challeng as non-cooperative behaviour always requires global blockchain interaction. The case study conducted by the KCL co-PI demonstrated a real-world example for state channels as it may be in the adversary's interest to force-close the state channel and force all parties to finish executing the smart contract entirely on the blockchain. Another difficulty is **how to extend state channels to more than two parties**. Multi-party state channels are possible, but several real-world problems must be resolved before they can be adopted. For example, state channels simply break down if more than one party proposes a state transition at the same time and as a result the application must be carefully designed to avoid race conditions. So far, there is no proposal for a **non-custodial sidechain that can support smart contracts**. The difficulty is how an honest party can prove to the global blockchain in a generic manner that a smart contract execution approved in the non-custodial sidechain was invalid. The final outstanding research challenge is **evaluating the incentive-compatible and strategy-proof mechanisms**. For both payments and smart contract off-chain execution, there is still no clear model or rigorous game-theoretic analysis.

5 Methodology and Work Programme

The project is split into three work packages. WP1 and WP3 will be lead by the KCL co-PI, whereas WP2 will be lead by the NCL co-PI.

5.1 WP1: Off-chain Protocols for Smart Contracts

In this work package, we focus on how to design off-chain protocols to support smart contract execution. This is broken down into three sub-tasks

which include how to support executing smart contracts within an off-chain solution, the outstanding research problems for designing a reliable watching service and how new blockchain protocols are required to better support off-chain smart contracts.

T1.1: Off-chain Smart Contract Execution. We focus on both scaling approaches (state channels and non-custodial sidechains) for executing smart contracts in an off-chain manner for this task.

We plan to address the problems we discussed earlier for state channel which focuses on reliability and performance while maintaining the same security guarantees. This includes investigating how to let multiple smart contracts within a state channel interact with each other in an off-chain manner, how to handle race conditions to support concurrent execution of smart contracts and how to handle time-critical events in the channel. Of course, while the above tasks rely on mechanism design (WP2) to ensure that parties honestly follow the protocol, it'll require re-thinking design paradigms for writing smart contracts for use within a state channel and this will be used as the basis for a new software framework (WP3).

On the other hand, the KCL co-PI's proposal Sprites was among the first to transit payment channels to support arbitrary smart contract execution within a state channel. We conjecture that a similar transition is possible for non-custodial sidechains as well. To do so, we'll investigate the current constructions for non-custodial payment sidechains including Plasma and NOCUST. Conceptually, the balance of parties in both proposals can be viewed as a simple application state. We believe our channel constructions from Sprites (and Kitsune) can be adopted to extend Plasma or NOCUST to support maintaining the state of an arbitrary smart contract. We will formally evaluate and prove the security of our design to ensure any new protocol is indeed non-custodial and every party is protected against a full collusion of all other parties.

T1.2 A Distributed Watching Service. All off-chain protocols introduce a new undesirable assumption that parties must remain online and fully synchronised with the network. We will continue to investigate and build PISA, our accountable third-party watching service, to help alleivate the always online assumption. PISA is currently designed as a single watching service, and we plan to extend it in several ways to increase its resilence and to let independent watchers collaborate without trusting each other. This new architecture involves designing a single (and not trusted) coordinater who interacts with the customer and a set of watchers. The co-ordinator sends all watchers a job request from the customer and the signed receipt is only valid if k of n watchers have accepted it. This increases the resilence of PISA as an adversary will need to take down at least k independent watchers to defeat PISA. We will also evaluate whether a set of watchers can collaborate in an incentive-compatible way in WP2.

T1.3 New Blockchain Protocols

We plan to design a new blockchain architecture with the aim to support off-chain protocols out of the box. This task is essential due to the difficulties witnessed in existing blockchains so far. For example, it is not feasible to design non-custodial sidechains that operate on top of Bitcoin due to its limited programming mechanism, and it is non-trivial to instantiate a smart contract within an Ethereum state channel (i.e. install an app in an off-chain manner) without it first being deployed in the underlying blockchain. To alleviate the above problems, we plan to focus on how to simplify the process for parties to authorise the execution of a smart contract off-chain and whether new transaction formats are required for better managing the dispute process via the blockchain.

Short-term network congestion (e.g. in the events of Status ICO and Cryptokitty launch) has previously caused the network's transaction fees to spike to unaffordable levels. In the worst case, a spike in transaction fees can prevent an honest party triggering (or resolving) a disagreement for an off-chain protocol via the blockchain. Thus an adversary can take advantage of network congestion to withdraw more coins than they deserve as it is not cost-effective for an honest party to challenge it. We'll investigate a new mechanism to let a blockchain detect congestion and let the blockchain extend the dispute process if it was indeed congested. Furthermore in WP2 we'll evaluate the financial cost for the network's maintainers to try and influence the mechanism.

5.2 WP2: Crypto-economics for Off-chain Protocols

While off-chain protocols aim to protect honest parties by letting them fairly resolve disputes and attribute responsibilities, there is still a financial cost for resolving dispute that we must consider. First, if the cost of resolution is higher than the amount being disputed (e.g. due to a spike in transaction fees), an honest part may rather accept the loss than resolve the dispute. Secondly, the more frequent the disputes are, the more resources in the global blockchain will be consumed, which is in contrary to our scaling goal. Therefore, we need to compensate honest parties fairly and deter/disincentivize malicious behaviour (so that disputes can be minimized). To achieve the goal, we need a mechanism that adjust and evaluate the financial pay-

offs in order to induce rational self-interested parties to cooperate (behave in an honest manner). There are three tasks in this WP:

T2.1: Game modelling. There are multiple parties in an off-chain solution as described in WP1, including e.g. the parties using the off-chain solution, the off-chain solution operator (i.e. sidechains) and a watching service to protect offline parties. Each party has its own interest and possible strategies. To understand their incentives, we will need to build a game-theoretical model and analyse their strategic decisions to ensure no one can take advantage of the others. Obviously, information asymmetry plays an important role here. We will start by modelling in terms of an incomplete information game [4] where parties keep their preferred outcome secret and their actions may be hidden from others. We must consider multiple iterations of this game, and investigate different ways of modelling interaction. We could use perfect public ex post equilibria [3] for example to model and analyse the repeated game in which the players' actions may not be directly observable. Our partners will support us in examining real-world use cases for state channels, the constraints provided by our partners and how this will impact the games we model.

T2.2: Mechanisms The game model will help us to understand the issues around the dispute process. e.g. should parties be punished for publishing an older state? Or should we simply let the blockchain accept the latest state? Does punishment encourage good behaviour? Can it result in new attack vectors (i.e. doesn't easily aid with crash recovery). Then based on the model, we can design mechanisms to redistribute funds and disincentivise malicious behaviour, which will be integrated to the services and protocols developed in WP1. As well, we have mentioned a few tasks in WP1, which we will aim to address here. Generally, we will design incentive structures and rules of reward/punishment to shape the strategies of the parties, e.g. deposit, tax, insurance, lottery or guarantors. Ideally, we aim to find an optimal mechanism that gives us the desirable outcome where the dominant strategy for all parties is honest behaviour. We will tune the mechanism with domain knowledge provided by our partners. If this is too hard and weaker guarantee is admissible, we will also consider approximation mechanisms that is approximately optimal. We will adopt recent development in Baysian mechanism design [6] to cope with the complexity brought by uncertainty and the large number of players.

T2.3 Interplay with cryptography. We will consider the interplay between economic mechanisms and cryptography. Cryptography is effective in terms of enforcing preventive controls that forbid malicious behaviours and this has an impact on mechanism design as it eliminates certain strategies. For example, a party cannot impersonate another because it cannot produce a valid digital signature. There are more advanced cryptographic protocols and algorithms such as zk-SNARKs [5](a type of zero-knowledge proof protocol), being proposed for use in blockchains. They hold the potential to ensure all disputes have a constant cost regardless of the smart contract (or its execution), while enhancing the privacy of smart contracts executed within the state channel. This is important for us to consider as it will potentially simplify the game between parties and make the mechanism design easier [7]. On the other hand, when designing a mechanism, we can actively incorporate cryptographic protocols to reduce the assumptions and strengthen the guarantee. That said, cryptographic protocols can also introduce a large computational overhead, which needs to be taken into account. We will investigate how to make trade-offs and strike a balance.

5.3 WP3: Software Framework and Impact Generation

In this work package, we focus on how the research project will produce a software framework that can be adopted by application developers to support off-chain solutions. As well, we'll focus on how our research can generate impact with our partners null and the null. Finally we'll highlight how our research will impact the wider cryptocurrency and blockchain community.

T3.1 Software Framework for Cryptocurrency Eco-system.

In this task, we will focus on the design and implementation of a state channel development framework, to facilitate application developers building off-chain solutions. It should provide an abstraction so application developers can still design the logic for a smart contract without the need to be concerned about the off-chain solution. Alongside the support of our partners, we'll open-source the software framework and refine it over several iterations with real-world application developers. Potentially, the framework can be blockchain agnostic so it is compatible with Ethereum and the emerging cryptocurrencies which include Dfinity, Cardano, etc.

6 National Importance

Blockchain has been one of the most visible technologies in the last a few years because it creates the potential for major disruption. In a January 2016 report [1] from the UK Government Office for Science,

[1] https://www.gov.uk/government/publications/distributed-ledger-technology-

it already recommended a broad government effort to explore and test blockchain and distributed ledger technology. In the UK Digital Strategy for 2017[2], it listed "applications of blockchain and smart contracts" as one of the key technologies the government will focus on moving forward. Our project aligns well with the government's strategy and will contribute to realising the government's vision of making the UK the world-leading digital economy.

Despite the growing interest in Blockchain, it is still a nascent research topic in the very early stages of exploration. As a result, we have seen a surge in R&D investment around the world related to Blockchain. In the UK, there have been several Blockchain research projects funded by the EPSRC and InnovateUK. Many of those projects focuses on exploring transformative use cases of Blockchain, and will benefit from our project because scalability is the most significant roadblocker of Blockchain applications.

Our project falls under the ICT and digital economy themes, and addresses priorities in those themes, such as"new and emerging areas in ICT", "safe and secure ICT" and "trust, identity, privacy and security".

7 Academic Impact

Scalabitilty is a fundamental problem in blockchain research. The techniques developed in this project could be ultimately adopted by the next generation blockchain platform. So this research proposal has the potential to impact everyone working in this area. This proposal could also have broad impact on researchers in communities such as cyber security, distributed systems, cryptography, and economics, as we will provide new insights on consensus, cyprtographic constructions, incentives, and how they jointly affect trustworthiness of a complex system. To max out impact, we will publish in top venues and attending conferences, organising workshops and have close collobaration with top researchers in this field (including ***). More details can be found in the academic beneficiaries in the form.

8 Management

The workpackages have been planned to achieve a balance risk and ambition within them. To leverage all possible insights, the workpackages will be executed in close connection. However, to reduce risk in relation to dependencies there is sufficient scope within each workpackage to enable it to independently proceed even if another one id hindered by unforeseen circumstances. In order to foster closer collaboration, the RAs will spend two weeks at the other institution each year, and we also planned research visits to overseas academic partners. We will manage the project by: 1) research group meetings to provide regular opportunities to report on progress, generate new ideas, and integrate the RAs into the local environments; 2) setup a slack channel and have skype meeting regularly to discuss technical and management matters; 3) 6-monthly project meetings; 4) asking our partners to review our progress each year.

blackett-review

[2] https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy

References

[1] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In *IEEE SP*, 2015.

[2] J. Dilley, A. Poelstra, J. Wilkins, M. Piekarska, B. Gorlick, and M. Friedenbach. Strong federations: An interoperable blockchain solution to centralized third party risks. *CoRR*, abs/1612.05491, 2016.

[3] D. Fudenberg and Y. Yamamoto. Repeated games where the payoffs and monitoring structure are unknown. *Econometrica*, 2010.

[4] O. Grandstrand. Games with incomplete information: the general model. In M. Maschler, E. Solan, and S. Zamir, editors, *Game Thoery*, chapter 10. Cambridge University Press, 2013.

[5] J. Groth. On the size of pairing-based non-interactive arguments. In *EUROCRYPT*, 2016.

[6] J. D. Hartline. Bayesian mechanism design. *Foundations and Trends in Theoretical Computer Science*, 2013.

[7] J. Katz. Bridging game theory and cryptography: Recent results and future directions. In *TCC*, 2008.

[8] R. Khalil and A. Gervais. NOCUST - A non-custodial 2nd-layer financial intermediary. *IACR ePrint*, 2018.

[9] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford. Omniledger: A secure, scale-out, decentralized ledger via sharding. In *IEEE SP*, 2018.

[10] S. D. Lerner. Rsk: Bitcoin powered smart contracts, 2019.

[11] Y. Lewenberg, Y. Sompolinsky, and A. Zohar. Inclusive block chain protocols. In *FC*, 2015.

[12] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2009.

[13] R. Pass and E. Shi. Thunderella: Blockchains with optimistic instant confirmation. In *EUROCRYPT*, 2018.

[14] J. Poon and V. Buterin. Plasma: Scalable autonomous smart contracts, 2017.

[15] N. Szabo. Formalizing and securing relationships on public networks, 1997.

[16] G. Wood. Ethereum: A secure decentralized transaction ledger, 2014.