Tracer: Peer-to-Peer Finance

Ryan Garner, Lachlan Webb
Mycelium

Jason Potts, Chris Berg, Sinclair Davidson
RMIT University

Version 1.3
June 28, 2021

Abstract

In this paper we introduce Tracer: peer-to-peer financial infrastructure for the decentralised economy. Tracer lowers the costs of participating in financial markets, using blockchain technology to enforce property rights and settle financial contracts without the need for a trusted third party. Tracer's Factory smart contract hosts an ecosystem of standardised financial contracts. Tracer DAO can install proposed contract templates into the Factory, which can be accessed and deployed by anyone with a connection to the Internet. Once deployed, a contract is permissionless and not subject to DAO governance unless specified. A Reputation System allows users to identify financial risk and assess under-collateralised financial opportunities. Oracle financing is introduced as a novel model that incentivises the discovery and standardisation of new data for use in decentralised financial contracts. Tracer's financial infrastructure stands to be the backbone of a secure, global financial network and provides strong foundations for future financial innovation.

Contents

Introduction

The current financial system relies on trusted third parties to facilitate transactions. Spot, derivative and lending market software currently meets most users' demand, yet still leaves them exposed to unnecessary costs and risks associated with third party control. Access to markets can be censored by financial software providers, blocking market participation. Software downtime (due to failure, maintenance or third party intervention) prevents users from conducting critical, time-sensitive transactions. Financial innovation is stifled due to high bureaucratic costs, inefficient legacy technology and a lack of clear standardisation around product creation. Transaction costs are high and can take up to several days to settle due to legacy clearing and settlement infrastructure. Information regarding counterparty risk is non-transparent, leading to financial insecurity for all participants. Trusted third parties can be completely removed from financial contracts and transactions by leveraging blockchain technology to enable an environment for a more efficient financial system.

Tracer is a peer-to-peer financial software network that does not rely on a trusted third party. The Tracer Factory is a smart contract that can be used to host, modify and deploy censorship resistant financial contracts that permit markets with absolute uptime. Once a financial contract is deployed from the Factory, it is permissionless, low cost and allows for its users to clear their transactions within seconds. The management of the Factory, including incentives for new market discovery and innovation, falls under the governance of Tracer DAO. A secure oracle framework is utilised for dynamic financial contracts, and an oracle financing mechanism is proposed to discover and standardise data for use in markets. All financial transactions and contracts are open-source, catering for a Reputation System that provides security insights into the risk of specific markets and counterparty risk. Privacy-preservation is permitted for those not willing to reveal their trading strategy and a front-running mitigation service can be utilised to provide transaction fairness. With this technology, Tracer intends to serve as a tool that enables a globally-connected and secure peer-to-peer financial system.

Robust Markets and Good Derivatives

Global financial innovation has greatly accelerated over the last century, in large part due to technological advancements in communications and computing. A variety of financial products derived from interest rates, government bonds and ecosystem assets (such as carbon) were pioneered to serve market demands and provide people with meaningful methods of risk management. The creation of new products has historically been expensive due to the high cost of coordinating involved actors. Tracer proposes a system that allows actors to coordinate financial innovation through simple, transparent and efficient contractual architecture.

The value of financial innovation can only be realised if the costs of establishing and operating a market do not exceed the benefits [1]. Given Tracer's low cost framework, financial contracts can be created when demand for a spot market exists, clear property rights are present and there is standardisation of contracts. Spot market volumes are simple to observe on public blockchains and interest for new spot markets can be gauged by cheap, immutable signals. Clearly defined property rights are codified in transparent smart contracts and the ownership of assets can be proved without trusting a counterparty. To achieve contract standardisation, financial contracts are replicable and quick to deploy, which allows markets to adopt the most effective contracts. Any upgrades to contract terms can be decided by, and displayed to, users. With these conditions many

new financial contracts can be engineered. With Tracer:

- Global ecosystem markets can be standardised, allowing the creation of derivative products that provide price insurance and hedging mechanisms for essential commodities such as water and atmosphere. Such markets enable firms to hedge their risk when offsetting environmental costs with the purchase of ecosystem assets.
- Derivative markets can form around non-fungible tokens (NFTs) which include rare art and in-game items. These markets enable artistic creators and in-game players to hedge against their asset risk, and also use their assets as security for lending.
- Microlending structures can allow individuals to issue credit lines and repackage their debts. Trustless mechanisms can be installed into contracts to liquidate any collateral and guarantee instant payment in cases of default.
- Programmable indexes and managed fund structures allow individuals to map their market beliefs to an investment or derivative position. Bundles of stocks, commodities, rare art and land can be packaged in a form that aligns with an individual's preferences.

The Factory

Peer-to-peer financial contracts can be created in the Tracer Factory. The Factory is a smart contract that allows for financial contracts to be installed, modified and deployed to the market. The Factory's name originates from a design pattern known in software engineering as the 'factory method'. In Tracer's context, this pattern allows any financial contract to be installed as a template. Factory contracts can then be deployed without permission in a modular, efficient manner.

Contract standardisation enables scalability. Once a financial contract has been installed into the Factory, all terms and conditions specified within the code are transparent. Market participants can view the rules of the Tracer contracts in which they deal, and, if they feel the rules are unsuitable, propose changes to the contract. On top of this, software maintenance and financial contract upgrades can be conducted without affecting online markets, which guarantees 100% uptime for market participants.

A Perpetual Swap will be the first financial contract considered for installation. A Perpetual Swap is an agreement that allows two parties to go long and short on any underlying asset, for any amount of time. The Tracer Perpetual Swap contract, and its mechanisms, are explained in a separate paper.

The Factory is structured to provide incentives for innovation. Each new financial contract added to the Factory may provide clear remuneration terms for its creator or modifier. Dynamic incentive packages can be structured around financial contract transaction fees, market usage or other quantifiable metrics. Each contract added to the Factory benefits from the network effects of the Tracer ecosystem.

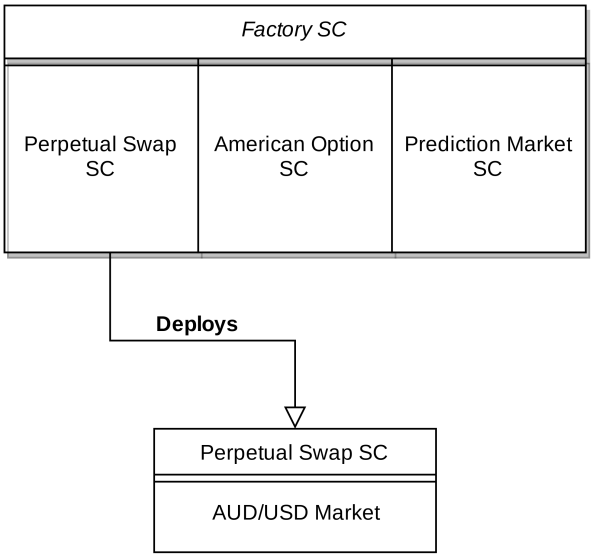

FIGURE 1: The Perpetual Swap smart contract (SC), American Option SC and Prediction Market SC templates have been installed into the Factory SC. A Perpetual Swap SC is deployed, requiring no permission; the deployer provides contract inputs such as the AUD/USD market.

Tracer DAO

Tracer is owned and governed by a Decentralised Autonomous Organisation (DAO). A DAO is a collection of smart contracts deployed as unstoppable code on blockchain platforms such as Ethereum [2]. DAOs can be engineered to form a corporation or any organisational structure. Participants of Tracer DAO can create proposals that:

- Maintain and upgrade Tracer smart contracts;
- Contract and remunerate service providers; and
- Manage any network incentive programs.

DAOs are the cheapest, most transparent and most secure way to achieve cooperation and incentive alignment for a globally connected financial software protocol. Much like corporations, the DAO will grant stakeholders certain governance rights according to the DAO Constitution. The approval of a proposal may require a majority, a super-majority or a consensus, depending on predetermined conditions embedded in the DAO contract. Also embedded in the DAO contract is the DAO Participation Agreement, which establishes the rights and obligations of TCR token holders, service providers to Tracer DAO and other participants engaging with Tracer DAO.

The acceptance of a vote that targets any piece of software within the Tracer system will automatically update that software in real-time. For example, a vote to modify an interest rate variable of a financial contract in the Factory, upon passing, has an immediate effect on the contract. In this way, DAO governors can serve similar functions to software engineers.

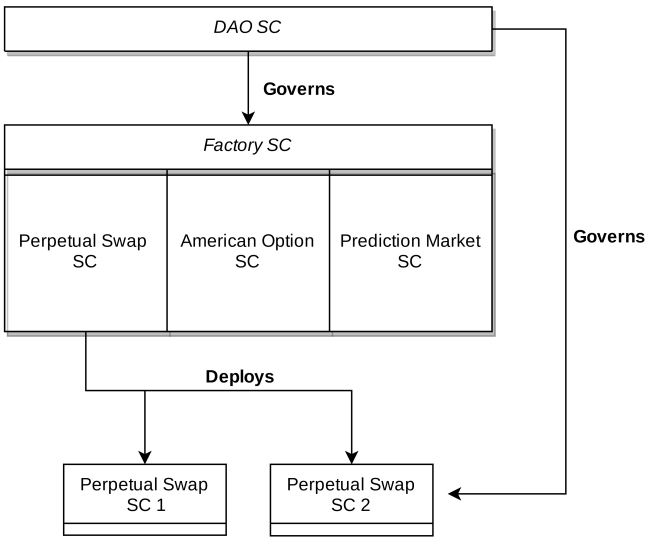

FIGURE 2: Perpetual Swap SC 1 selects to be independent of DAO governance and Perpetual Swap SC 2 selects to be DAO governed.

While Tracer DAO controls the Factory, it may not control deployed financial contracts. Deployed contracts are not subject to DAO governance unless the deployer of the contract expressly consents to it. Markets can be governance free; they are designed to be modular and contain clear, immutable parameters. This design enables trustless peer-to-peer trade without the need for third-party exchange or DAO governance.

Commitment voting

TCR token holders have the right to vote in DAO proposals. Most DAO voting mechanisms use a one-token, one-vote structure which too often results in a small number of token holders dominating governance, with a corresponding reduction in representative and quality governance decisions. Tracer DAO will utilise a novel voting mechanism called commitment voting which allows for voters to signal their intensity of preference and compete with voters that hold large amounts of tokens [3]. In commitment voting, the weight of a token holder's vote is a function of the number of tokens under their control multiplied by a nominated lockup time, subject to a decay function. Tokens are released from lockup if they vote on the losing side. By empowering token holders in this way, commitment voting encourages high quality governance decisions and long term commitment to the DAO.

Oracles

A globally connected financial software protocol offering dynamic markets requires oracles to function. An oracle is a piece of middleware that allows smart contracts to connect to external data feeds and interact with systems outside of the blockchain environment. An example application of an oracle is a gold futures smart contract that requires an input (the price of gold) in order to settle and clear funds. Tracer's oracles:

- Provide price feeds and real-world data (e.g. weather data) to support financial contracts;
- Perform expensive computations that are infeasible on-chain;
- Perform dispute resolution; and
- Perform work outside of the blockchain environment, such as automation.

The need for reliable oracles cannot be overstated. Poorly engineered oracle frameworks lead to oracle attacks on financial contracts which, in the past, have seized hundreds of millions of dollars in value. A futures contract that requires the price of gold can be exploited if one party bribes the oracle to report the price in their favour. The oracle may also fail to report the price of gold if it ceases to function.

A decentralised oracle network guarantees accurate pricing, robust security and fair settlement [4]. The aggregate of the data provided by a network of oracles almost entirely mitigates the issues of corruption and poor performance through game-theoretic models that reward and punish behaviour at an individual oracle level.

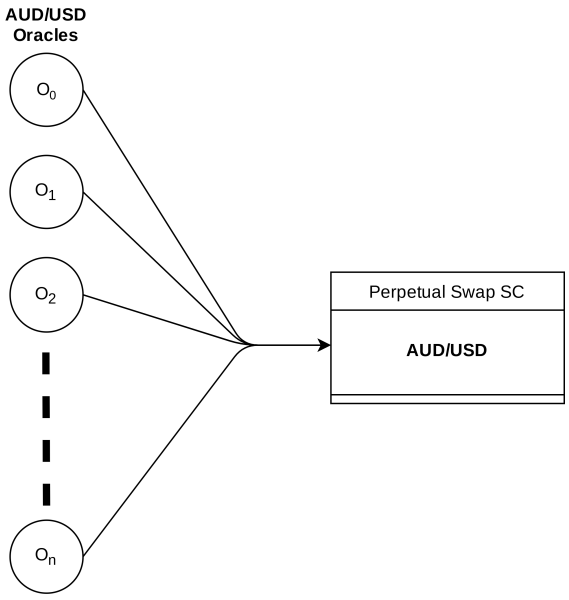

FIGURE 3: A contract pulls and receives price data from a set of oracles

To ensure that financial contracts are secure, Tracer contract deployers must remain oracle-agnostic and select oracle providers that have the best security and reputation. To choose the best oracles, contract deployers can utilise oracle reputation services that transparently display the quality of oracles [5].

Oracle Financing

In circumstances where deployers cannot source reputable or secure data feeds for financial contracts, Tracer introduces an oracle financing scheme. Oracle financing is the process of remunerating oracles for costs associated with data discovery. For example, a local fuel derivative market would require local fuel prices to function. In the absence

of a pre-existing, sophisticated and reputable data market for fuel, oracles would be enlisted by the market creator to discover and standardise such a market. Tracer Factory templates incorporate oracle financing models.

Reputation System

In traditional finance, credit ratings are given to financial products and market actors as a measure of risk. The failure of rating agencies at the turn of the millennium resulted in the Global Financial Crisis. Traditional risk rating systems failed for a few reasons. Risk auditing is both a tedious and expensive process. Traditional financial products are complex and their information storage (multiple databases and/or large paper trails) makes them difficult to analyse. Closed environments also give rise to information asymmetries, which allow financial actors to collude to produce inaccurate ratings favourable to them. Open source standards resolve many of the issues associated with auditing by making data available for update and review.

Tracer's Reputation System enables transparent and cost-effective risk assessment within a peer-to-peer financial ecosystem. Reputation Scores that reflect traditional credit scores can be generated by analysing open-source financial contract and transaction data. Scores can be used to assess the risk of financial contracts and individual market agents. On-chain data used to form a Reputation Score may include:

- Number of transactions;
- Transaction volume;
- Oracle reputation;
- Collateralisation ratios; and
- Contract specifications.

The integrated Reputation System can accept a combination of the above information, and other information, to generate different reputation metrics. The information used to provide a Reputation Score for a financial contract can be different from the information used for an individual interacting with that contract. Reputation Scores should be designed for transparency, objectivity and should leverage verifiable data. Tracer's Reputation System does not limit financial access for the individual. On the contrary, it simply provides a foundation for individual market participants to assess counterparty risk and engage in agreements that fit their risk profile.

System Design

Tracer is an adaptable piece of financial infrastructure that is able to evolve with developments in existing blockchains and other peer-to-peer transaction technologies. With that being said, Tracer's system design performs optimally in environments that are:

- Decentralised;
- Scalable;
- Secure; and
- Liquid.

Decentralised

Third party risk and its associated costs are mitigated through decentralisation. Ethereum is the initial Layer 1 blockchain that will support Tracer. The thousands of node operators that secure the Ethereum network guarantee decentralisation. Layer 2 solutions can be connected to the base transaction layer to achieve certain goals such as decreasing transaction time and cost, or providing privacy. The viability of deploying Tracer on another blockchain network (or Layer 2 solution) should be assessed in terms of decentralisation. If there is a risk of central control then Tracer should not be deployed.

Scalable

Tracer is best suited to networks that allow fast, cheap transactions. Scalability can be optimised at the blockchain level, the Layer 2 level or at the smart contract level. For Ethereum, Layer 1 sharding and Layer 2 Optimistic Rollups will bring enhanced speed and economy to transactions [6]. Smart contracts proposed to the DAO should be optimised for efficient computation and the DAO should only consider contracts that minimise cost. Implementations of cross-chain systems can enable transactions that support multi-chain DAO governance, allowing Tracer to scale across multiple networks [7].

Secure

Security is considered and achieved at the platform, smart contract and oracle level. If the security of the underlying blockchain is compromised, Tracer is able to migrate its software to a more suitable chain. Only invulnerable smart contracts should be installed into the Factory, ensuring that the logic within the contracts does not put user funds at risk. Tracer DAO must perform security checks before adding new financial contracts to the Factory or migrating to other Layer 1 or Layer 2 platforms, in order to continue to achieve optimal security. As an additional oracle security measure, smart contract code can be engineered to protect users' funds in the event of oracle failure. For example, a smart contract can detect if the input value is 50% greater than the most recently observed price. This detection can trigger a market freeze which can then be resolved using a bonded oracle dispute mechanism [8].

Liquid

At the time of writing, the Ethereum network holds the most liquidity of any turing-complete blockchain. Many financial primitives such as lending, borrowing and exchange already exist as financial contracts on Ethereum. Tracer contracts can leverage existing liquidity and utilise other smart contacts to create highly liquid, interconnected financial markets. Evolving Layer 1 and Layer 2 bridging solutions will allow for the seamless and cheap flow of liquidity between blockchains. With such technology, and other cross-chain transaction mechanisms [9], assets that are exclusively traded on one blockchain can be utilised in financial contracts on another blockchain, maximising Tracer's access to liquidity.

Transaction Types

Open, observable transactions pose privacy and front-running problems. Software solutions that can be utilised within the Tracer system address these concerns and provide additional ways to transact.

Privacy-preserving Transactions

Many over-the-counter (OTC) agreements and trade deals are settled with confidentiality. Most financial actors, intermediaries and banks do not wish to reveal their strategy to the market. Tracer contract users that do not seek to disclose their transaction details and wish to preserve their financial privacy will have the option to do so. Transaction mixing protocols [10, 11] and privacy layers can help users achieve this preference for privacy [12].

These solutions implement various cryptographic techniques that allow users to transact with the same benefits that open networks offer. Standardisation around privacy will continue to emerge and Tracer DAO is incentivised to respect the right to privacy in order to maximise user options.

Front-running Prevention

Front-running is derived from open outcry trading floors where a trader would indicate their preference to purchase a stock, the indication of which would provoke another trader (the front-runner) to jump the stock purchasing line and position themselves in front of the initial trader. This front-runner can then sell the stock to the initial trader for a small profit. Blockchain networks emulate this open outcry environment, thereby leaving the door open to front-runners. In order for a transaction to be placed in a block there must be a small transaction fee that compensates miners or validators who maintain the blockchain. In this environment, front-runners will compete with each other, increasing the transaction cost one bid at a time [13].

One way to mitigate front-running is for financial contracts to accept orders from a Fair Sequencing Service (FSS) [14]. A Fair Sequencing Service is provided by decentralised oracle networks, which receive, compute and report a 'fair batch' of orders to an on-chain smart contract. Tracer contract creators should only utilise a service such as FSS if the oracle network is sufficiently decentralised. Other methods of mitigating front-running include the use of on-chain commit-reveal schemes and anonymity sets [15]. Further research and applications that emerge to solve front-running issues should be explored by Tracer DAO.

TCR Governance Token

A Tracer governance token (TCR) is a token that grants its holder the ability to participate in voting on proposals that influence Tracer. There are 1 billion TCR tokens to be distributed by Tracer DAO over time. An initial 1% of TCR tokens have been claimed by 100 globally distributed members who will discuss and vote to allocate the remaining 99% of tokens. The remaining 99% of tokens are likely to be allocated, by Tracer DAO, to software developers, financial engineers, market participants and any other members that could provide value for the future of Tracer through governance participation. The Tracer Governance framework, and its constitution, are explained in a separate paper.

Conclusion

The peer-to-peer financial network proposed by Tracer is an important step toward empowering the individual's financial agency and achieving a robust global financial network that places the individual at the heart of its interest. We discuss the Tracer Factory, which can be used to host, modify and deploy financial contracts, enabling global permissionless access to finance. Tracer DAO and TCR tokens are utilised as a means to govern the Factory and align network incentives to optimise financial contracts. The Reputation System introduced allows for the fair assessment of counterparty and financial contract risk. A secure oracle network, and the introduction of oracle financing, allows for quality external data to reach Tracer financial contracts. Tracer's system design is optimised for decentralisation, security, scalability and liquidity, allowing it to service the needs of a globally connected financial system.

References

[1] Richard L. Sandor. Good Derivatives: A Story of Financial and Environmental Innovation. John Wiley & Sons, Inc., 2012. ISBN: 9780470949733. DOI: 10.1002/9781119201069.

[2] Vitalik Buterin. Ethereum Whitepaper. 2013. URL: https://ethereum.org/en/whitepaper/#notes-and-further-reading.

[3] Chris Berg, Sinclair Davidson, and Jason Potts. "Commitment Voting: A Mechanism for Intensity of Preference Revelation and Long-Term Commitment in Blockchain Governance". In: SSRN Electronic Journal (2020). DOI: 10.2139\ssrn.3742435.

[4] Steve Ellis, Ari Juels, and Sergey Nazarov. Chainlink Whitepaper. 2017. URL: https://link.smartcontract.com/whitepaper.

[5] Chainlink Oracle Reputation. Reputation.link. 2019. URL: https://reputation.link/contracts.

[6] EthHub. Optimistic Rollups. 2019. URL: https://docs.ethhub.io/ethereum-roadmap/layer-2-scaling/optimistic_rollups/.

[7] Peter Robinson and Raghavendra Ramesh. General Purpose Atomic Crosschain Transactions. 2020. arXiv: 2011.12783 [cs.CR].

[8] Luis Cuende and Jorge Izquierdo. Aragon Network: A decentralised infrastructure for value exchange. 2017. URL: https://github.com/aragon/whitepaper.

[9] Peter Robinson et al. Atomic Crosschain Transactions for Ethereum Private Sidechains. 2019. arXiv: 1904.12079 [cs.CR].

[10] Ari Juels et al. Mixicles: Simple Private Decentralized Finance. 2019. URL: https://assets.website-files.com/5f44d690acb168953e6181f6/5fa2f1616ac1b092226b3a86_mixicles.pdf.

[11] Alexey Pertsev, Roman Semenov, and Roman Storm. Tornado cash Whitepaper. 2019. URL: https://tornado.cash/Tornado.cash_whitepaper_v1.4.pdf.

[12] Zachary J. Williamson. The AZTEC Protocol. 2018. URL: https://github.com/AztecProtocol/AZTEC/blob/master/AZTEC.pdf.

[13] Philip Daian et al. Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges. 2019. arXiv: 1904.05234 [cs.CR].

[14] Ari Juels, Lorenz Breidenbach, and Florian Tramèr. Fair Sequencing Services: Enabling a Provably Fair DeFi Ecosystem. 2020. URL: https://blog.chain.link/chainlink-fair-sequencing-services-enabling-a-provably-fair-defi-ecosystem/.

[15] Lorenz Breidenbach et al. To Sink Frontrunners, Send in the Submarines. 2017. URL: https://hackingdistributed.com/2017/08/28/submarine-sends/.