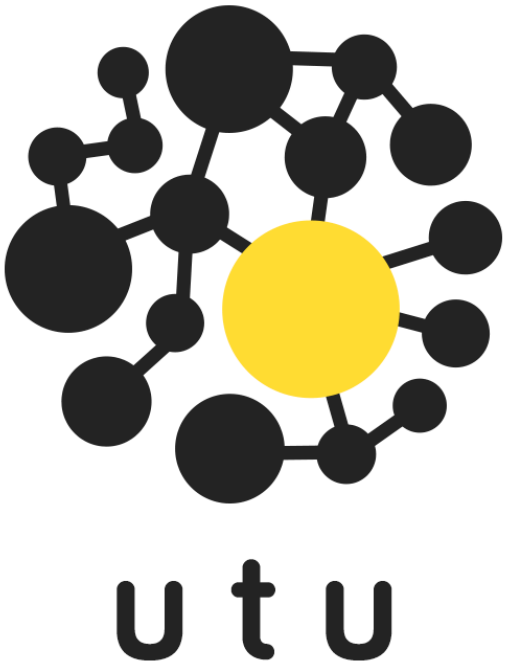


Enabling DeFi

UTU PROTOCOL RADICALLY TRANSFORMS DEFI ECONOMICS AND EXPANDS THE REACH OF THE SECTOR

Context

- Extending FinTech use cases to remove the current requirement of 100% trustlessness, while providing a mechanism to establish the then-required trust.
- In DeFi, the majority of lending is overcollateralized; UTU's idea is that adding a trust layer will reduce collateralization requirements
- By participating in the platform via endorsing (or disapproving) oracles, users will earn UTU Coins. Possession of UTU Coins gives them voting rights for governance of the UTU Trust mechanism. Votes can be (re-)delegated similar to Liquid Democracy or other currently applied DeFi governance mechanisms like Compound's.

- UTU Protocol further rewards participation in the protocol by awarding UTU Trust Tokens. In short, these are awarded for providing truthful (and therefore trustworthy) feedback and other data to the platform. Please refer to our whitepaper for details how these are structured such that truthful behaviour is incentivised.

Trustlessness (or not) in Defi

Un/collateralised Lending

For a long time, credit offering institutions such as banks have evaluated the creditworthiness of consumers based on traditional credit scoring methods that rely on an individual's or business's financial history. Factors such as how regularly one settles bills, how many credit accounts they have open, history of delinquency, and the length of a person's credit history, are reduced to a single score that determines not only whether you get credit, but also dictates the terms of that credit. However, the lack of these data points in Decentralized Finance burdens borrowers significantly with high collateral amounts and interest rates. This not only requires large collateral amounts to access the loans, it also locks up liquidity for the borrower.

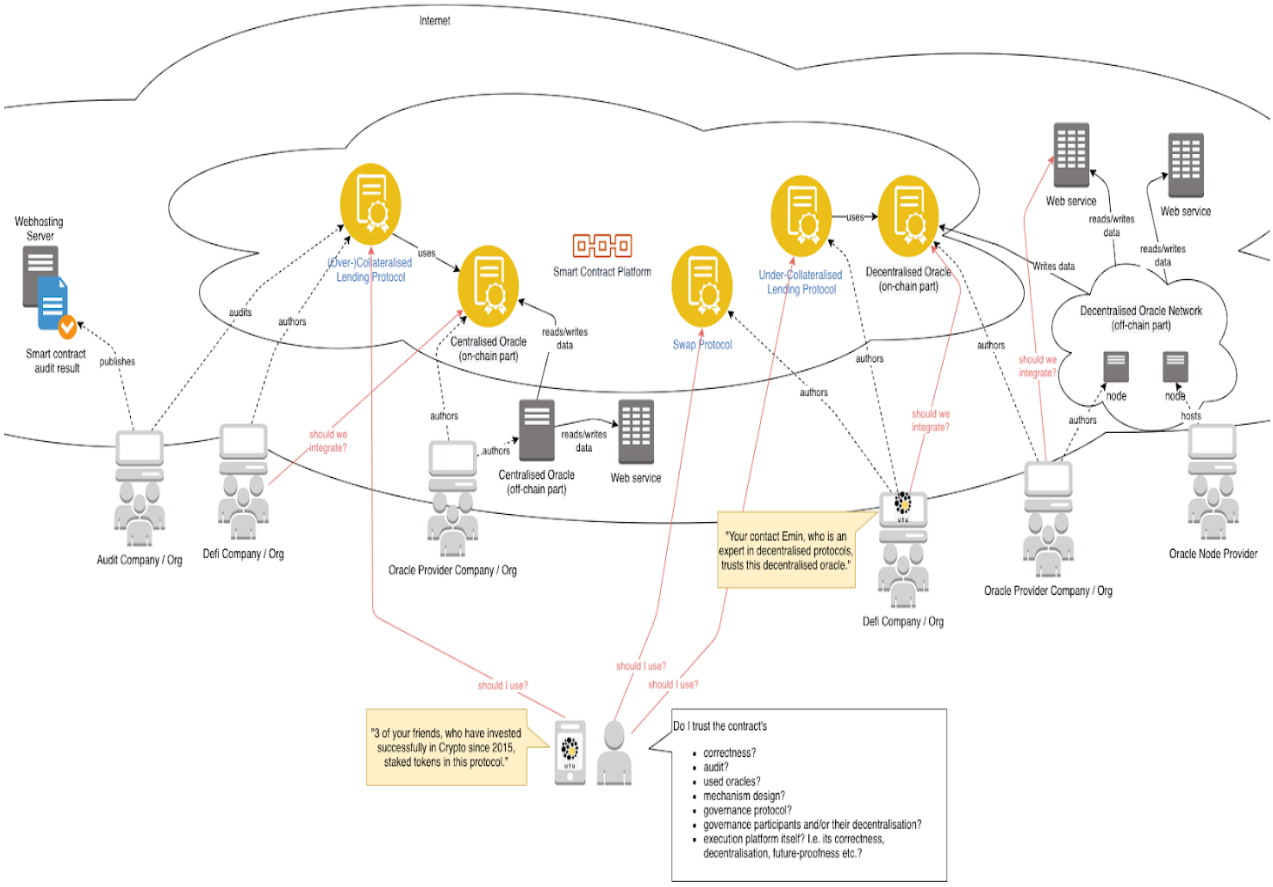
To overcome this, various techniques have recently been suggested, including the application of traditional as well as more advanced forms of credit scores. Different such credit scoring or assessment methods would be provided to on-chain DeFi protocols via oracles.

However, such techniques come with different advantages and drawbacks, and consequently different risk profiles. In addition, the best models are often highly context-sensitive and domain-specific, as we learnt at UTU while developing some of such models (see UTU Powers FinTech for a few concrete examples below).

Trust Requirements in Basic DeFi Infrastructure

But even DeFi protocols such as MakerDAO or Compound themselves, while purportedly trustless, in fact also require a certain amount of trust from their users. This is because "trustless" here means that a smart contract is technically correctly executed as-is on the given platform, such as Ethereum. However, this doesn't include many aspects that are still relevant for an actual user to trust in the whole system and process.

The following figure depicts some of the components and parties typically involved in DeFi protocols, and we discuss their trust aspects in the following subsections.



Smart Contract Code

While a well-functioning smart contract platform executes smart contracts truthfully according to their code (rather than executing something else), this doesn't mean that the code itself necessarily implements what a given protocol promises its users. I.e. if the code contains bugs, even if it is executed correctly, this can still be catastrophic for users. A recent example is failure of the YAM protocol, which ended in large losses for their users.

To mitigate this risk, better managed protocols employ techniques such as formal verification (still quite rarely to our knowledge), auditing and rigorous testing. But even then, mistakes can still be made:

- Formal verification provides a proof that a system (here smart contract) strictly adheres to its formal specification. However the specification itself might be incorrect or incomplete, or it might not implement exactly what a user expects after reading advertisements and documentation of a protocol. This might happen because of misunderstandings, a lack of domain knowledge of the user, etc.
- Auditing is usually done by human experts, who analyse the code and provide an auditing report. However this then requires users to trust the work of the auditors,

their expertise, diligence etc. Also, misunderstandings of what a given protocol is supposed to do in all cases can still still happen.
- Testing runs the code in a test environment for a number of test scenarios. However whether these cover all possible situations and invocations is often hard to see in complex systems. Here, the user has to trust that the test authors did not overlook anything.

We note that smart contracts are typically open source, and so a technically knowledgeable user might theoretically execute all of these strategies themselves. However, most potential users lack some or most of this knowledge, and so have to trust others on their opinion whether a given protocol is safe to use and does what they think it promises, be it the developers, auditors, or technically knowledgeable acquaintances.

Oracles

Oracles provide an interface from smart contract code to the off-chain world, e.g. to retrieve some data from some web service. DeFi protocols often use some form of price oracle to determine the current market price of some token. In under-collateralised lending, credit scoring and similar services might be employed.

In any case, using an oracle means that a smart contract invocation depends on data outside the trustless execution realm, and therefore becomes trustful by definition. The question then becomes whether the user trusts the involved oracles and off-chain services.

On Ethereum, Oracles typically consist of two components: an on-chain smart contract, which might be invoked from other smart contracts as well as the oracle's off-chain component, which interfaces to external services.

Therefore, the trust caveats noted in the previous section also apply to the on-chain part of oracles. The off-chain parts can fail in different ways: the oracle's own off-chain interface might be faulty or buggs, or a used malicious web service might provide false data. Both might also simply become unavailable.

Part of this problem is solved by decentralised oracles such as provided by the Chainlink protocol. However, the user then still needs to trust the decentralised oracle's architecture, correct specification, execution etc. Some of the same caveats with respect to trustability as for smart contracts as well as platforms (see section Smart Contract Platform below) apply.

Apart from decentralising the off-chain component of the oracle itself, protocols such as Chainlink propose to use multiple data sources and aggregate their responses to determine any single point of data. They also provide a few default aggregation strategies (such as simple averaging, possibly with removal of outliers), but leave more complex strategy implementations to the oracle operator. Whether a given strategy protects against all possible failure scenarios in a given protocol and set of oracle data sources (or sinks) depends on the concrete use case and its domain. Ultimately, a user who is not both

technically knowledgeable enough and a domain expert will still have to trust that the oracle provider is doing the right thing, or rely on a trusted third party to assure them of the same.

Protocol Design

Even if the smart contract code and used oracles were completely trustworthy, i.e. implementing a specified protocol correctly, are live, reliable etc., there might still be issues with the protocol design itself. Such issues might be more or less obvious, and techniques such as game-theoretic mechanism design can be used to devise incentive-compatible protocols (which however is often difficult in complex settings).

Even then, such techniques often (have to) make certain underlying assumptions, such as that the underlying smart contract platform works within a certain range of "normal" parameters at all times.

This then can lead to situations such as the recent MakerDAO meltdown on "Black Thursday", where a crash of the value of ETH triggered automated auctioning-off of collateral in MakerDAO pools. Hackers then placed 0-DAI bids on the auctions and flooded the Ethereum mempool (where yet-to-be-processed transactions are queued) to prevent other bid transactions from being processed.

This was in effect an exploit of a weakness of the MakerDAO auto-auction protocol, which materialised only in unusual circumstances, but could nonetheless have been prevented by different protocol parameters. Indeed, MakerDAO changed the rules of the game following this. But is the protocol now safe against other supposedly rare events?

Ultimately, most users are no experts in protocol design, game theory or mechanism design etc., and will have to rely on the opinion of trusted experts.

Governance

Nowadays most d-app protocols are upgradable, meaning that e.g. on Ethereum, they use a pattern of multiple connected smart contracts which allows replacing parts of the protocol by deploying new smart contracts and updating their references in others. Upgrades are necessary to adapt protocol parameters, fix bugs and generally evolve a protocol over time.

When a protocol is first launched, this upgrading can usually be done only by the originating author or organisation. In this situation, users have to fully trust them, because they might change the protocol at any time. Therefore this situation requires a large amount of trust by users.

OTOH, over time many protocols switch to a decentralised governance model, often implementing weighted voting protocols according to the amounts of the protocol's own tokens that users staked. While this removes the dependency on the protocol's original

authors or administrators, it does not prevent a single user or colluding group of users to obtain enough tokens to effectively take over the protocol.

We have already seen that centralisation and 51% attacks are a problem in all but the largest blockchains. So it's not hard to imagine that often much smaller (in terms of capital requirement) DeFi protocols become a target here, likely opening new ways of exploits for attackers.

So here the user has to trust not only the governance mechanism itself, but also that the protocol will draw a large enough and diverse base of users who take part in the governance.

Smart Contract Platform

Finally, users need to trust in the well functioning of the platform which runs a protocol's smart contract itself, and in the current DeFi world this means Ethereum. However, particularly Ethereum has had its share of hacks in the past, mostly around quirks in its smart contract language solidity.

While this situation has arguably improved over time, both through improvements in the language and a growing body of knowledge and techniques to make smart contracts less bug-prone (though the above-mentioned caveats apply), there are still more potential problems, such as a lack of scalability.

We already discussed the recent attack on MakerDAO by flooding the Ethereum mempool, so effectively a kind of DOS attack. But also the ever rising fees, ultimately caused by Ethereum's low transaction capacity, pose a serious risk to the current DeFi landscape.

While there are mitigations in the works, they are either still quite far off (Ethereum 2.0 will likely still take a few years) or add more complexity to an already complex system, such as using techniques like state channels, optimistic rollups or side chains.

Again, particularly non-technical users will likely rely on their trusted known experts' opinions whether they should move any money onto a platform which does not seem riskless at all, from a higher perspective.

Bringing Trust to the Trustless

As the previous sections show, there are in fact many places where current and future DeFi protocols do rely on trust, despite their claim of being trustless. To alleviate this, UTU's trusted recommendation mechanism and creditworthiness methods built on top of this can help in three distinct ways:

UTU's Credit Trust Oracles

UTU introduces new and unique ways to determine a borrower's creditworthiness using our trust infrastructure that accesses contextually relevant on- as well as off-chain data to provide trusted creditworthiness assessments.

UTU's trust oracles can assess a borrower's creditworthiness using data from social graphs and other contextual factors. With this additional layer of trust, DeFi borrowers can borrow by providing lower collateral amounts. Moreover, UTU's recommendation engine can allow both lenders and borrowers to better assess the other party and therefore make a more secure decision. This will also allow lenders to lend on their own terms, rather than those pre-defined by existing platforms such as Compound.

So far with experience deploying UTU trust infrastructure on off-chain projects (but working on support for on-chain projects as well), our trust recommendation technology uses available contextual data such as mobile money transactions to provide an additional layer of credit check. The underlying models are typically domain-specific, and we refer to the below section "UTU Powers FinTech" for a few concrete examples.

UTU will make these mechanisms available via oracles to support upcoming DeFi lending protocols to support under-collateralized loans, thereby enabling access to borrowers who cannot afford collateral in the first place.

UTU's Recommendations for Credit Scoring/-worthiness Oracles

Assuming that a number of credit scoring/-worthiness oracles are available, should a given lending protocol support? Should each user be able to choose their own set? How would they make that choice? This is another layer where our trusted recommendation mechanism can be employed.

This enables users to endorse oracles as trustworthy (or not), and other users and protocol builders can review such endorsements from users they trust. Specifically, this will enable P2P lending where each lender can decide which oracles and borrowers they trust to which degree, and therefore which amount of collateral and which interest rate to require. In other words, this establishes a fully decentralised P2P reputation mechanism for creditworthiness.

Relying on on-chain endorsements of services and providers, in this case oracles, users don't need to take our word for it -- they can verify that our recommendations are truthful (including that we don't fraudulently recommend our own oracles over others when this is not warranted by the underlying endorsements).

UTU's Recommendations for DeFi Protocols and Infrastructure

UTU's trust layer can also be applied to help users choose which DeFi protocols they want to interact with, by showing respective recommendations in DeFi portal apps. We might integrate with such apps, but also build UTU's own DeFi portal app.

This will enable users to identify DeFi protocols (and generally any DAPPs) that fit their unique requirements. In this way, UTU provides a mechanism to close the trust gaps that still exist despite the technical trustlessness of the smart contract execution layer.

UTU Powers FinTech

UTU is already working with these great fintech companies to bring better trust to digital financial services:

P2P Lending with ShuttleOne and Jamborow

Jamborow and ShuttleOne both run blockchain-based lending P2P lending platforms that are transforming access to financial services across Africa and SouthEast Asia respectively. UTU is working with these companies to provide our trust infrastructure services to their platforms for better credit scoring using diverse ranges of datasets and custom-built AI tools.

Crypto Credit Scoring with CredMark

Credmark is filling a giant hole in the emerging crypto financial system, providing the credit data that will allow this financial system to function well. Without data, credit can't exist. Credmark is producing this data. UTU and Credmark have been collaborating since 2019 to unite and harmonize our services and deliver ever more valuable credit information.

Tokenomics

UTU's trust infrastructure comprises two native tokens, the UTU Token (UTT) & the UTU Coin (UTU), each serving a different purpose.

UTU Trust Token (UTT)

The UTU Trust Tokens will act as a non-transferable utility token. Intuitively, clients will be rewarded for active participation in the system with UTU Tokens. They can be used to make staked endorsements and access trusted recommendations provided by the UTU

Recommendation Service and other services. The token will be non-transferable to prevent people "buying into" the network, essentially buying trust. Users who employ UTU trust oracles will allow them to endorse (or disapprove of) other oracles, lenders or borrowers by staking UTU tokens and will also earn UTU token on successful endorsements. Possession of UTU Token gives them voting rights for governance of the UTU Trust mechanism.

There are 2 main avenues of earning UTU tokens:

1) Providing data into the UTU ecosystem (including data from social networks, phone-books, M-Pesa transactions etc.) This data collection will enable UTU to provide trusted recommendations on creditworthiness and can help decrease collateralization.
2) Making staked service endorsements on borrowers or oracles

If an endorsement leads to a recommendation by UTU's service and is shown to another user that also endorses this same service provider, the original endorser will be rewarded additional tokens for having successfully recommended a provider. The reward depends on both endorsers' stakes and some system parameters, bounded by a maximum fraction of the service fee of 10% (which makes it irrational to try and consume services for the only purpose of being rewarded tokens). To level the playing field between holders of many ("whales") and those of few tokens, the reward function implements diminishing returns for increased stakes.

UTU Coin (UTU)

UTU Coin will be accepted as a form of payment within the UTU ecosystem of applications, by third party platforms and DAPPS. It will be required to use our trusted recommendation service, and to pay users who demand it for accessing their data. We target the UTU Coin to be slightly deflationary, as to provide value for its holders. However, being freely tradable, its value will be determined by the market.

UTU's own services will accept fee payment in UTU Coin, and we will encourage other services on the platform to accept it. This might be implemented via discounts on the fees to use our recommendation service, or even as a requirement for the same.

One might obtain UTU Coin in these ways:

1) By actively taking part by providing data and endorse services and then converting some of the awarded UTU Trust Tokens to UTU Coin (see following sections),
2) Selling access to one's data to UTU's recommendation as well as other interested parties, like 3rd-party services on the platform,
3) Taking part in token generation/distribution events and
4) By trading on exchanges for other coins, tokens, or fiat money.

To make UTU Coin deflationary, the total available amount over all time has to be bounded, similar to Bitcoin.