




Trustology × *gunnercooke*

Peering into the depths of DeFi:

Know Your Code

How Dirty is Your Pool?



DeFi DApps, or decentralised autonomous financial application services, are attracting the attention of institutional investors and service providers alike e.g. funds focused on DeFi yield, brokers sourcing liquidity from decentralised exchanges (DEXs), etc. But such DApps are neither individuals nor organisations, so how on earth do you stay compliant with AML regulations? In this article, UK based challenger law firm gunnercooke and crypto custodian Trustology share their perspectives.

Regulation of DeFi: A legal perspective on AML

No one argues with the general principle that criminals should be prevented from seeking to hide illicit gains, or that terrorism should not be financed. The issue, rather, is how to counteract this activity under changing circumstances i.e. AML rules were originally created in the context of industries where a core part of providing a service involved a face-to-face relationship with the client, something which is no longer true. With DeFi protocols, such as those underlying Uniswap, one of the largest decentralised crypto exchanges or DEXs in the world, it is now entirely possible to trade crypto-assets on a decentralised basis without there being the traditional business / client relationship i.e. counterparties are anonymous and

intermediaries are replaced by autonomous code.

Whilst technological inventions typically disrupt the status quo, regulation, on the other hand, builds on precedent and principles: the first thing a lawyer does is look to see what has happened before, and builds on this to develop the legal and regulatory framework. As such, lawyers do not “invent” law, rather they adapt the existing framework to accommodate changes, and even then the starting point is generally simply to slot the invention into the existing rules, rather than to create rules for the invention. Indeed, the concept of creating specific law for new technologies has historically met a sceptic response,

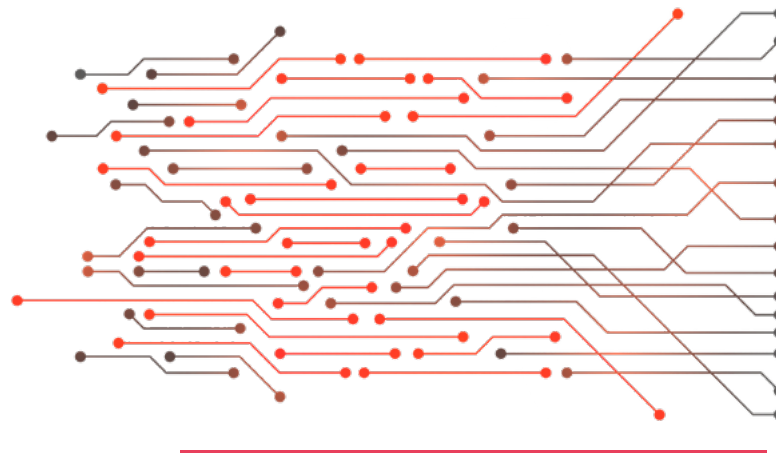
being likened by Easterbrook to creating a “law for the horse”.

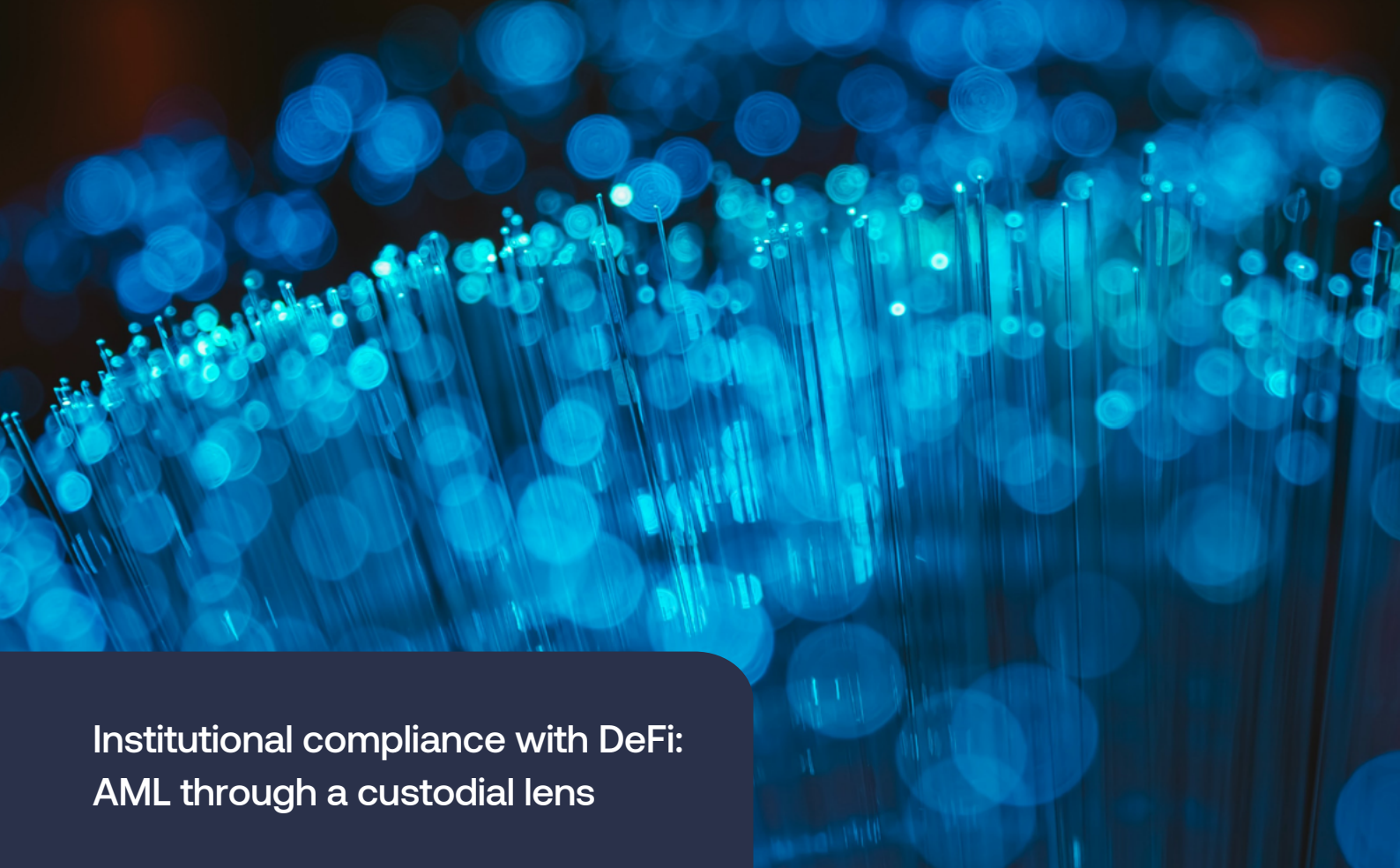
Using a technology neutral to rule development as a starting point makes sense and ensures a consistent approach rather than new rules proliferating every time there is an “innovation”. However, there is a balance to be struck. Rules which are too abstract start to look like principles, and principles can be vague. For example, one of

the core principles endorsed by the UK Financial Conduct Authority is that “a firm must pay due regard to the interests of its customers and treat them fairly.” Whilst as a statement this is fairly undisputable, it will not always be clear what is actually meant by having “due regard” to someone’s interest and what, in a particular scenario, is acting “fairly”. Indeed, clarifying what is desirable behaviour is the driving force behind a vast amount of regulation. The issue here, then, becomes how law is clarified. In other words, any level of clarification has to make inherent assumptions regarding the activity being clarified. And in this case, the activity is the use of DeFi DApps in an AML compliant manner. The following section proposes one such possible clarification.

Lots of cases deal with sales of horses; others deal with people kicked by horses; still more deal with the licensing and racing of horses, or with the care veterinarians give to horses, or with prizes at horse shows. Any effort to collect these strands into a course on ‘The Law of the Horse’ is doomed to be shallow and to miss unifying principles.

Easterbrook, Frank H. (1996).
“Cyberspace and the Law of the Horse”,
University of Chicago Legal Forum





Institutional compliance with DeFi: AML through a custodial lens

Since the introduction of the 5th AML Directive in 2020, UK based custodian wallet providers like Trustology, must comply with Money Laundering Regulations i.e., conduct customer due diligence (CDD) based on Know Your Customer (KYC) standards, and perform ongoing monitoring of customer transactions and changes in customer circumstances. Additionally, as a custodial wallet platform capable of supporting DeFi DApps via MetaMask and WalletConnect integrations, they needed to grapple with how this could work, as decentralisation and anonymity are the cornerstones of DeFi.

They began with the basics. As cryptoasset transaction counterparties may be anonymous, regulators accepted a risk-based approach to compliance. In practical terms, blockchain analysis tools like Chainalysis or Elliptic are used to identify if the counterparty's account address is known by them to be high-risk. If so, the transaction must be investigated and possibly quarantined.

Traditionally, accounts are controlled by either individuals or organisations. On blockchains like Ethereum, however, accounts can also be controlled by DeFi DApp's smart contract code. Like any financial service, these DApps can be exploited by criminals and terrorists to avoid AML and CFT controls.

To counter, it is helpful to deal with DApps in much the same way one would deal with individuals and organisations i.e. use a risk-based approach. Hence, the custodian needs to KYC the DApp. Clearly, there are no individuals or UBOs that can be screened, but there is code to assess for the level of inherent risk associated with code's activity, in order to risk rate the DApp.



For example, a decentralised exchange (DEX) DApp that relies on liquidity pools, is inherently more risky than for example an atomic swap smart contract enforcing an OTC payment-versus-payment settlement transaction. Why this is the case is because cryptoassets from illegal sources can be easily combined with those from legitimate sources in a pooled DEX to avoid AML/CFT controls i.e. layering. Also, some DApps will only allow cryptoassets to be sent back to the sender's address, whilst others allow forwarding of cryptoassets to third party addresses such as UniSwap. This introduces new money laundering or terrorist financing vectors.

Higher risk DApps should be subject to enhanced ongoing monitoring to adjust their risk rating based on their usage e.g. DEX's liquidity pools must be measured for percentage of funds that came from addresses associated with darknet markets.

This way it is possible to treat a DApp's account as any other, i.e., transactions from or to high-risk DApp accounts, either direct or forwarded, that should be investigated and possibly quarantined.

The problem with this approach is that DApps have no way to protect themselves from misuse by criminals or terrorists. A DEX's liquidity pool can be polluted by anyone sending funds from a darknet address. And what was a great source of liquidity becomes tainted and unusable. A possible solution is for DApps to involve whitelisters like custodial wallet providers, who will KYC pool participants.

Concluding thoughts

It is easy to criticise the AML rules as imperfect for a DeFi model, but the solution is not to ignore them – to do so risks tarnishing the reputation of DeFi technologies as illegitimate. Rather, the key is, in addition to complying with the existing rules, to show how, using new innovation, alternative approaches such as custodians are possible

which better meet the underlying aims of the rules. Doing this as best practice casts the DeFi industry in a positive light and encourages the level of trust needed from lawmakers to encourage them to consider whether they should adapt rules in light of changing assumptions. It is easy to criticise, anyone can do that. The challenge is to create something better.

→ About Trustology

We make it safer, faster and easier for institutions to securely hold crypto assets and handle any financial transaction on-chain and on-exchange.

www.trustology.io

→ About gunnercooke

We are a challenger law firm with experienced practitioners advising blockchain, digital asset and FinTech enterprises.

www.gunnercooke.com

