Feature

**KEY POINTS**

- Interoperability describes the ability of computer systems or software to exchange and make use of information – in the context of blockchains this means how different blockchains communicate with each other.
- The internet solved the interoperability problem of siloed computer networks, but what will solve the interoperability problem of blockchains? Nobody knows for sure what it will be, but perhaps we will call it the "interchain".
- Lawyers who understand crypto-specific laws as well as the current decentralised ecosystem and infrastructure are required as trusted advisors to entities and governments of all sizes but they will need to regularly update their understanding as we move closer to the interchain.
- As decentralised finance becomes more interoperable and secure, more stakeholders will enter the industry and traditional finance entities will find it necessary to plug-in via standardised on-ramps and off-ramps to remain relevant.
- Once the infrastructure connecting blockchains is standardised, we will see less exploits of security vulnerabilities and regulation will become easier.

**Author** Tom Marshall

# Blockchain interoperability: connecting decentralised infrastructure for traditional finance

In this article, Tom Marshall explains the meaning of interoperability in the context of blockchains, existing infrastructure and why and how traditional finance is getting involved.

## INTRODUCTION

The early internet: If you were interested in data communications for computer networks in the 1960s and onwards, you would have come across several siloed networks such as the NPL network, APRANET, Merit Network, CYCLADES, X.25 and UUCP. Each network had its own, albeit small, community in various parts of the world with differing methods for connecting. Clearly, solving the fundamental problem of internetworking was required to unify these networks – today we call this solution the "internet" and it is facilitated by a common protocol (a system of standardised rules) named "TCP/IP". TCP/IP lets you send emails, watch Netflix or get directions on your smart phone – you do not think about it, but it is a key part of the infrastructure that sits behind your seamless customer experience.

Where do smart contracts fit in here? Expecting communications for computer networks to not continue to evolve beyond TCP/IP would be natural, but perhaps misplaced. Smart contract platforms built on distributed ledger technology provide a trustless, transparent and secure alternative system for communicating with the potential for superior efficiency to TCP/IP facilitated internet activity. The problem is these smart contract platforms are not interconnected by a system of standardised rules. Until this problem is solved, these platforms and the communities that have formed around them, will operate in silos. This is not a problem if you interact with just one blockchain, but for traditional finance entities (such as retail banks, credit unions, brokerage firms, insurance companies and central banks) to offer seamless customer experiences or for governments seeking to deliver seamless public services, infrastructure, facilitating an interoperable multichain ecosystem will be required. This will allow their customers to communicate, interact and transact with each other in a secure, convenient, timely and cost-effective manner.

Just like the evolution towards the internet as we know it today created both opportunities and challenges for lawyers, so too will the journey to blockchain interoperability. Before there can be a system of standardised rules connecting blockchains, traditional finance entities will require trusted advisors to understand cross-chain infrastructure solutions, including sidechains, bridges, atomic swaps, oracles and "network of networks" projects (see below). The opportunity lies in understanding these solutions, but the challenge is keeping up with the rate of change, all while preparing for unification through standardisation.

## BODY 1: WHAT IS INTEROPERABILITY IN THE CONTEXT OF BLOCKCHAINS?

Several different blockchain platforms (eg Ethereum, Solana) have come to the fore over recent years, each with their own advantages and disadvantages – some with different fee amounts, transaction times, throughput, security or the degree of decentralisation. But what happens when data or cryptoassets need to be transferred from one blockchain to another? How can value on one chain be transferred to another chain?

In practical terms, interoperability allows users, developers and applications to operate on top of multiple blockchain platforms, meaning a wide range of functionalities within a broad multi-chain ecosystem. So, whilst blockchains will continue to be built for specialised ideas (such as the Flow blockchain which was developed

primarily to handle billions of consumer NFT transactions), mass adoption may not be achieved until we reach a period of "interconnected blockchains". Perhaps, just like the internet, this interconnection will have its own name (eg the interchain) and so persons will not so much conduct their activity "within a blockchain" but rather by just using the "interchain".

Certainly, with more complex applications being explored, cross-chain interoperability standards will be increasingly needed, and these standards will need to consider blockchain specific technical topics such as platforms, applications, data exchange, wallets and key management.[1] Significant standardisation efforts on these topics have been made already and is best summarised by the World Economic Forum, in collaboration with other members of the Global Blockchain Council. Together they have set out standard setting initiatives by groups such as the International Organisation for Standardisation in Switzerland looking at identity, the Enterprise Ethereum Alliance in the US looking at interoperability and tokens and the National Blockchain Distributed Accounting Technology Standardization Technical Committee in China looking at DLT requirements and DLT terminology.[2]

These standardisation efforts are a step towards the "interchain", but it's clear that interoperability cannot result from the efforts of a single entity and rather it requires all stakeholders working together under a governance framework.[3] Before we get there though, it's important to understand the existing infrastructure facilitating the current form of interoperability between blockchains.

## BODY 2: EXISTING INFRASTRUCTURE

So, how do we get different cryptoassets, relying on different tech stacks and protocols with different market requirements and compliance standards to communicate with one another? At the moment, the answer is a complex array of technical solutions all patching different parts of a fragmented ecosystem together. Here is a quick summary of those solutions.

### Sidechains

Sidechains are a type of layer-2 scaling solution (meaning a network that operates on top of a blockchain to increase its scalability and efficiency), with their own blockchain network compatible with a single layer-1 main chain. Typically, a sidechain improves a layer-1's processing efficiency by allowing cryptoassets to be transferred back and forth between the mainchain and the sidechain. Technically, the "transfer" of the cryptoasset never occurs as they are locked on the mainchain while the equivalent amount is unlocked in the sidechain – which requires verification by a smart contract. This effectively increases transaction throughput dramatically while also sacrificing security by not being recorded directly to the main chain.

### Cross-chain bridges

Bridges between blockchains facilitate a connection that allows the transfer of tokens and/or arbitrary data from one chain to another. Both chains can have different protocols, rules and governance models, but the bridge provides a way for people to communicate between them. Bridges are either centralised (trusted) or decentralised (trustless). The difference is explained by looking at who controls the tokens that are used to create the bridged assets. For example, all wrapped bitcoin (WBTC) – a digital token representing Bitcoin on the Ethereum network – is held in custody by BitGo – a digital asset trust and security company – (as well as the key to mint more of it), making it a centralised bridge. However, bridged assets on Wormhole[4] – a portal bridge which allows you to bridge tokens across different chains (mainly used between Ethereum and Solana) – where the original token gets locked in a smart contract on the protocol and a new portal wrapped token gets minted on the target chain, are (at least more) decentralised. There are fundamental limits to the security of bridges though – in January an attacker exploited a vulnerability in Wormhole to create for themselves 120,000 wrapped Ether coins worth $320m and in March there was a breach of the Ronin network bridge to the NFT game "Axie Infinity" for 173,600 Ethereum and 25.5 million USD Coins (USDC) worth $625m. Together these breaches total almost US$1bn.

### Cross-chain atomic swaps

Just like currency exchange services facilitate trading pounds for dollars in the traditional finance system, atomic swaps facilitate an exchange of tokens across chains (there's just no central entity which assists you with the exchange). The swaps are "atomic" because they are "all or nothing", both sides succeed or the entire transaction reverts. For atomic swaps to work across blockchains, both blockchains need some kind of relative timelock operation (like OP_CHECKSEQUENCEVERIFY), as well as the ability to hash data and check that date against a given hash.

### Oracles

Oracles – being entities that connect blockchains to external systems, thereby enabling smart contracts to execute based upon inputs and outputs from the real world – especially decentralised oracle networks, play a fundamental role in decentralisation. Their necessity is brought about by the limitations of blockchain networks – which cannot fetch external data or send data to off-chain systems. If it were not for oracles, such as those offered by oracle node operators within Chainlink – the leading decentralised blockchain oracle network – the only way for data to enter blockchain environments would be via centralised entities (eg a person entering the price of gold into a smart contract at a computer). This would render smart contracts within those environments subject to tampering and invalidates any decentralisation that blockchains offer.

By using a decentralised oracle network, which aggregate multiple data inputs, smart contracts can be connected to real-world data, events, payments, verifiable randomness, keeper functions, external APIs and off-chain

computation in a tamper-resistant manner. Therefore, any smart contracts with inputs from these oracles will be hybrid in nature – because they do not just have code running on a blockchain, they also have data and computation from outside the blockchain.[5] If it is to succeed, the interchain will need hybrid smart contracts.

Now that we know a bit more about the current technical solutions for blockchain interoperability, let's take a quick look at how traditional finance can plug in and get going.

## BODY 3: WHY TRADITIONAL FINANCE IS JUMPING IN

Sending money, entering the lottery, buying insurance, paying tax, reviewing accommodation, health records and file storage – all these activities and more are going on chain (ie being put on the blockchain). To access and provide related products and services, traditional finance entities will want to plug-in to infrastructure that offers their customers the type of seamless customer experience with which they have become accustomed to.

However, plugging in is challenging for a number of reasons, not least because it disregards a unique feature of cryptoassets – that they are independent of the traditional banking system. Whilst this quality may have been a key reason that propelled cryptoassets into the public sphere, the relationship they have with the traditional banking system is unlikely to stay as unconnected in the future. This is due, in no small part, to the categorisation of cryptoassets as property under law in a number of jurisdictions.

In the UK, the UK Jurisdiction Taskforce (UKJT) has set out that cryptoassets should be categorised as property under English law. In their Joint Statement, they say that cryptoassets are:

(i) definable;
(ii) identifiable by third parties;
(iii) capable in their nature of assumption by third parties; and
(iv) have some degree of permanence (being the four criteria set out in Lord Wilberforce's definition of property in *National Provincial Bank v Ainsworth* [1965] 1 AC 1175).

Whilst the UKJT does not enact legislation or decide on case law, the statements have been echoed in English courts such as in *Fetch.ai Ltd v Persons Unknown* [2021] EWHC 2254 (Comm) where Pelling J stated he was satisfied cryptoassets were property under English law and in *DPP v Briedis* [2021] EWHC 3155 (Admin) where McGowan J came to the same conclusion. Further, the UK High Court has ruled in *Lavinia Deborah Osbourne v (1) Persons Unknown (2) Ozone Networks Inc Trading as Opensea* [2022] that NFTs are considered property and that a victim of NFT theft could have their stolen assets frozen through a court injunction.

This categorisation means that traditional entities can adapt their business models around a concept they are all too familiar with already – ownership. Ownership of cryptoassets may depend on the rules of the system in which they exist, but generally it can be determined by who has knowledge of a private key that controls those cryptoassets.[6] If something can be owned, then it can be sold and therein lies an opportunity exploited for millennia – finance.

## BODY 3: HOW TRADITIONAL FINANCE IS GETTING INVOLVED

For traditional finance entities looking to seize the opportunity, they will need blockchain tech savvy treasury, finance and legal teams or a relationship with a specialist third party service provider who has that capability. They will also need access to interfaces that communicate with blockchain nodes directly or through another service – application programming interfaces (APIs). So, software development expertise will be highly sought after.

Security will be key and so the use of institution compliant wallets (which is a non-custodial wallet that stores your cryptocurrency assets – Metamask Institutional is an example of an institutional service provider in this field) as well as permissioned DeFi platforms such as Aave Arc and secure staking platforms such as Codefi will be required. Additionally, custody of cryptoassets will be a challenge and many institutions will look to custody, trading, and settlement solutions providers such as Copper (other examples are Fireblocks and Anchorage) who are launching an institutional grade digital custody service where clients can store and settle their digital assets within a secure environment operated by State Street. [7]

But most importantly, to properly get involved, traditional finance entities will need to educate themselves on the interoperable infrastructure available to them so that they can operate in a way that maximises the reach of their offering. This means hiring subject matter experts, developing existing employees and working collaboratively with other organisations. However, they will need to be strategic about these decisions and make them with the future in mind – the interchain is just around the corner after all.

## BODY 4: THE INTERCHAIN

Blockchain interoperability, in its current form, is best understood by the existing infrastructure that facilitates smart contract activity across multiple blockchains. A system of standardised rules is yet to be developed; however, some projects are working to solve this fundamental networking problem and understanding them could hold the key for traditional finance entities. Here is a quick summary of those projects.

### Cross-Chain Interoperability Protocol (CCIP)

One solution, offered by Chainlink, is Cross-Chain Interoperability Protocol (CCIP) – being an open-sourced standard for developers to build secure cross-chain services and applications. With a universal messaging interface, CCIP eliminates the need for developers to write custom code for building chain-specific integrations and could play the role of TCP/IP for the new decentralised internet.[8] However, nothing is certain

*Biog box*

Tom Marshall is an associate at CMS. Tom plays a key role in CMS's crypto team advising clients such as Binance, Crypto.com, Kraken, Dapper Labs, Mutant Apes, Wirex as well as most of the top VCs and hedge funds in crypto including Outlier Ventures and Cointelligence. Having been an active member of the Ethereum and Chainlink communities for many years, he has developed a keen interest in on-chain analytics, unconventional valuation metrics and the challenges of good DAO governance. Tom previously worked at Samsung on several blockchain, artificial intelligence and technology projects. Email: thomas.marshall@cms-cmno.com

in a space subject to an exponential rate of change.

### Lightning Network

The Lightning Network is a layer-2 solution for Bitcoin's scalability issues and allows users to create peer-to-peer payment channels with one another. Opening a new channel requires a transaction on the main chain, but all other transactions are held off-chain until one party decides to close the channel, which then consolidates all transactions to the main chain. Many altcoin projects have adopted Lightning Network into their own networks, meaning cryptoassets can be swapped between two networks (eg swapping Bitcoin for Litecoin). We can think of the Lightning Network like taking a record of a zip folder on the main chain, rather than each individual file within the folder.

### "Network of networks" projects

Major projects such as Polkadot and Cosmos have been designed to be a comprehensive cross-chain infrastructure or "network of networks" meaning they have multiple chains which can communicate with each other via smart contracts.

Polkadot adopts a main chain, which it calls a "relay chain" that connects and supports various ancillary, application-specific blockchains, called "parachains", allowing for inter-chain communication and cross-chain transactions. Blocks are added to the relay chain only after parachains generate blocks for transaction validators on the relay chain, which provides network security. This is efficient, because different parachains can run parallel transactions without interfering with one another, meaning Polkadot can scale much faster than a traditional smart contract platform such as Ethereum.

## EXAMPLE: PLUGGING IN TO PAYMENTS – VISA

Perhaps unsurprisingly, the large payment processing networks are working in this space to identify (or perhaps create) a universal adapter among blockchains. Visa's solution is a framework for interoperability between different blockchain networks named the Universal Payment Channel (UPC). UPC would allow for dedicated payment channels to be established, so that perhaps a CBDC network could be connected to a private stablecoin network regardless of the blockchain either operates within.[9]

## CONCLUSION

Infrastructure connecting blockchains exists, but it will continue to develop as the industry becomes more connected. Once the infrastructure connecting blockchains is standardised, we will see less exploits of security vulnerabilities and regulation will become easier, but for traditional financial entities the time for action and education is now – if they want to remain relevant. I look forward to doing business with you on the interchain. ■

1 World Bank Document.
2 World Economic Forum Global Blockchain Council – Overview of Blockchain Technical Standards.
3 WEF_A_Framework_for_Blockchain_Interoperability_2020.pdf (weforum.org)
4 Portal Token Bridge (portalbridge.com).
5 Hybrid Smart Contracts Explained (chain.link).
6 Legal statement on cryptoassets and smart contracts (netdna-ssl.com).
7 State Street to develop digital custody in collaboration with Copper.co.
8 Cross-Chain Interoperability Protocol (CCIP) | Chainlink.
9 Making digital currency interoperable | Visa.

*Further Reading:*

- Digitised trading and settlement: Exchange 4.0 (2022) 3 JIBFL 176.
- Crypto yield (2022) 3 JIBFL 199.
- LexisPSL: Banking & Finance: Practice Note: Blockchain: key legal and regulatory issues.