THE STATE OF
BLOCKCHAIN 2023

MDRˣ

Contents

MDRx

A message from Tom Grogan

Welcome to the first of what will be going forward an annual MDRx State of Blockchain Report.

Blockchain technology has always been central to the MDRx offering. I have been heavily involved in the industry in various capacities since 2013, and MDRx's first engagements – long before we formally launched with our own brand, entity and bank account – were blockchain development and strategy projects. If you need a refresher on blockchain or are a newcomer, check out the Appendix to this Report.

Over the past decade, we have enjoyed and endured the ups and downs, met with triumph and despair, and fought for blockchain implementations rooted in value and utility rather than hype and noise. This year was no different, though it has felt like a watershed. This perhaps is surprising to read given the cryptoasset markets have been relatively flat and most of the headlines have been focussed on the trial of SBF who, shock, was found guilty on all counts. There has however been a hive of activity. Section 1 looks at some of the key brand entrants and exits, Section 2 summarises a few key trends and developments, and Section 3 views developments through the lens of business sectors. Section 4 looks at the key data summarising the crypto markets from January 2023 to 16th November 2023 when we locked the content for this Report.

In this first year, we choose to spotlight in Section 5 the unglamorous but critical subject of infrastructure, and preview progress made on account abstraction to improve UX. We also dive into some of the other barriers to adoption in Section 6 before making some of our own predictions for 2024 in Section 7.

Pulling this together has been a huge effort and I'm so grateful to my talented and dedicated team notably including Narcisa, Alex, Toba, Tari, Dulcie, and Omair. Thank you, and well done.

I hope you find this useful, and if you want to explore how blockchain can have application within your business, do get in touch.

Tom
CEO OF MDRX

1

Brand Watch

In this section, we look at some of the big brands that have entered, exited and doubled down on their use of blockchain technology through 2023.

Who's new?

The Premier League has followed the lead of La Liga and Bundesliga by partnering with Sorare to offer NFT digital cards of footballers for use within its fantasy football game, offering new and novel ways to engage with their fans. This builds on the many deals struck between Premier League clubs and Web 3.0 giant Socios, offering Fan Tokens which bring utility in various ways.

Citi, one of the world's largest and best-known banks, is leveraging blockchain technology to power programmable finance solutions including self-executing transactions. This, Citi hopes, can improve its turnaround times and therefore its customers' experience by offering 24/7 automated workflows provided pre-set criteria are met. This programmable finance is inching us ever closer to the "future of money" that the blockchain industry has long heralded and it is interesting to see it being driven by an established incumbent.

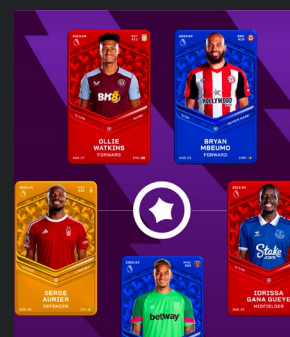Sorare offer NFT digital cards of football players. Credit: Sorare.com

Veloce plans to transform its consumer experience with Web 3.0 gaming, voting and staking. Credit: Veloce

Veloce, the world's largest motorsports and media company, is evolving its entire business to Web 3.0, handing over voting rights in respect of increasingly important decisions in the management of its business to its fans and integrating their native cryptoasset within a range of games and applications. This is an example of the "future of fandom" that we have long been promised, and it will be fascinating to see how an organisation that boasts over 700m monthly YouTube views and winning teams in high-profile real-world racing events leverages a new blockchain-based technology stack.

Who's out?

Chase UK joins TSB and digital bank Starling in banning the purchase of crypto assets on their debit cards or by transferring money to sites from Chase accounts. What seems like mixed messages (Chase UK's parent, US bank JP Morgan, is something of a blockchain pioneer through its corporate Onyx platform) might just reflect differing risk appetite in the back-office and the consumer market.

MDRx

Logan Paul, one of the world's most-watched YouTube influencers, promoted several crypto projects, including 'CryptoZoo', a platform to breed, collect, and trade exotic hybrid animals as NFTs. The penny has finally dropped – they are all pretty worthless now.

Youtuber Logan Paul has distanced himself from projects Credit: originals.com

Who's doubling down?

Reddit released the third and fourth generations of its collection of 'avatars', whilst Nike has partnered with EA Sports to "build new immersive experiences and unlock brand new levels of customisation in the gaming company's ecosystem".

The Starbucks Odyssey experience will offer members the ability to earn and buy collectible NFTs that unlock rewards and immersive coffee experiences. Credit: stories.starbucks.com

Mastercard expanded on its earlier Web 3.0 interest – it has a crypto card program – with the introduction of an Artist Accelerator incubator that will prepare emerging artists to "build (and own) their brand through Web 3.0 experiences like minting NFTs".

Although Telegram's own blockchain project fell foul of regulators in 2020, it has since allowed The Open Network Foundation (TON Foundation) to take the lead in an ecosystem that supports a growing number of blockchain applications on Telegram. In 2023, a third-party provider 'The Open Platform' (TOP) – yes, the acronyms have a theme – launched a 'wallet' enabling users to make in-app payments with a range of cryptoassets simply by sending messages to the 'wallet bot'.

Starbucks launched its NFT loyalty programme 'Odyssey' in December 2022 and has released a few thousand NFTs in 2023. The technology allows customers to collect NFT loyalty 'stamps', which they can redeem for surprise gifts, in effect offering lucky dip tickets that collectors can re-sell. Whether they prove to be a washout or the next big thing remains to be seen.

Who's working on it?

In September 2023, Sony, the multinational technology group, announced its rather bold intention to develop "a blockchain that can become the backbone of global Web 3.0 infrastructure" through a joint venture with Startale Labs. We await further details.

MDRˣ

The London Stock Exchange Group is also thinking big. They are taking forward plans to be the first major exchange to offer extensive trading of traditional financial assets on blockchain technology. Hopefully, they will learn from the rather painful failure of their Australian counterpart.

Continuing with the theme of financial institutions investing in blockchain, Swift, the international communication platform for the world's biggest banks, completed a series of experiments in August to prove that it could provide its services across different blockchains, a necessity if financial use cases for blockchain are to scale.

We round off Brand Watch with a final financial player: Blackrock, a giant asset manager, has applied to its regulator for a fund holding bitcoin that tracks the bitcoin price – a spot exchange-traded fund or ETF. They hope to succeed where others, so far, have failed. They certainly have the brand cache, industry nous and scale to pull it off.

Sota Watanabe is CEO at Startale Labs, working with Sony to develop new block-chain infrastructure. Source: startale.org

MDRˣ
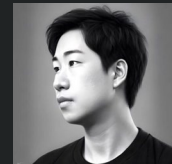
2

Trends and Developments

In this section, we take a look at the biggest stories, trends and developments that have touched and shaped the blockchain industry in 2023.

Biggest splashes: crypto legal dramas

COMPLIANCE BY DESIGN IS NO LONGER OPTIONAL

Blockchain has assembled an impressive cast of pantomime villains. Too often, what is really going on is wilfully obscured by "tech's next big thing", allowing crimes to grow into something quite sensational before they're uncovered. Unfortunately, these crimes are seldom victimless and the responses, from regulatory sanctions and new legislation to arrests and private legal actions, have scooped the lion's share of blockchain's headlines in 2023.

Co-founders of two separate cryptocurrency scams – the multi-billion dollar "OneCoin" scheme and "AirBit Club", have each been sentenced to more than 10 years in prison, while regulators have charged the companies and executives of Coinbase and Binance – the biggest names in the blockchain ecosystem. The collapse of one of blockchain's biggest success stories, the formerly multibillion-dollar company FTX, has been further scandalised after the SEC issued severe criminal charges against Samuel Bankman-Fried, its founder, and other executives. Bankman-Fried was convicted of five counts each carrying a maximum sentence of 20 years in prison and two further counts, carrying up to 5 years each.

It is not just public authorities making moves. There has been a flurry of private legal action, from copyright infringement to class actions in respect of OneCoin (being led by our Mishcon de Reya colleague Rebecca Belgrave and others) and Block.one frauds.

Gradually, the response is becoming more systemic and proactive, rather than simply reactive and targeted. In the UK, there are new crypto marketing rules and The EU has implemented its own regulatory framework, MiCA. Crypto's legal Wild West phase is approaching its end. Organisations leveraging blockchain technology will have to be compliant by design moving forward.
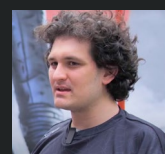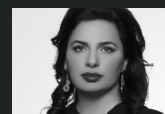
Some notable crypto convictions.

Pablo Renato Rodriguez, pictured (top) co-founder of the AirBit Club crypto membership scheme, was sentenced to 12 years. Credit: renato-rodriguez.io

Ruja Ignatova, pictured (middle) co-founder of the OneCoin crypto-currency scheme remains at large as one of the FBI's Top Ten Most Wanted. Her co-founder, Karl Greenwood, was sentenced to 20 years in prison in September 2023. Credit: Creative Commons

Sam Bankman-Fried, pictured (bottom), was convicted on seven criminal counts in November 2023 for his actions whilst CEO of blockchain exchange FTX, which dramat-ically collapsed in 2022. Credit: Creative Commons

MDRˣ

Read more about why MDRx welcomes this new regulatory interest in section 6 on the barriers to blockchain adoption.

Washout: NFT collectibles

NFTS, SHOCKINGLY, HAVE TO CARRY SOME UTILITY TO BE SUSTAINABLE

If you have been following blockchain news over the last few years, you probably do not want to read any more about the ever-growing number of almost comically preposterous NFT collections. Many appear to have been created cynically to make a quick buck. Others are just…downright weird (we are looking at you stoner cats).

Nevertheless, an eclectic set of big brands, from sports and luxury fashion to drinks companies and superhero franchises, have created, or committed to creating, NFT collections in 2023. Nike leads the pack with a history of impressive revenue numbers underpinned by solid and enticing utility, but many of the other big brands have only reached six figures from their collections – presumably marking losses.

Nike x RTFKT Dunk Genesis OG Edition
1/20000

3D FILES   PHYSICAL
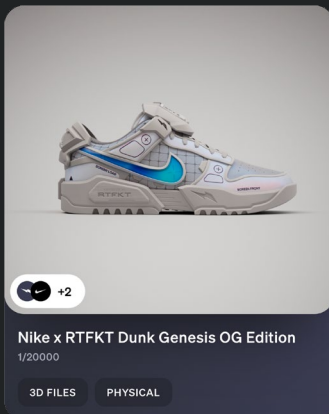
Nike launched NFTs featuring virtual apparel for avatars on its Web 3.0 platform .SWOOSH in May 2023. Credit: Nike

Of course, revenue is not the only reason to mint NFTs – consumer engagement can be the principal driver. However, with the number of collectibles necessarily limited to maintain scarcity, success is determined by engaging the highest-value consumers. And the best way of measuring their engagement? How much they are willing to pay. Whilst Nike and Adidas have managed impressive sales volumes, most brands have languished in the low $millions. Not amounts, you would imagine, their marketing directors will be particularly pleased with.

The picture over time is particularly sobering. The overwhelming majority of activity took place in 2021/22, before plummeting in the second quarter of 2022/23 and staying there, even for the likes of Nike. Estimates suggest that 79% of NFT collections have never sold anything – and 95% of NFT collections are worthless.

So, whilst some brands have made a success of their NFT ventures, that does not mean they have cracked it. The next chapter of the story might well depend on another set of technologies entirely: the Metaverse. For some

early collectors, knowing they own an NFT collectible might be enough. But the next billion might expect something more than a pathetic jpeg.

Might the integration of collectibles within and across collectors' digital journeys bring substance and style to the NFT market?

Choppy waters: the tough investment climate

GENERATIVE AI IS TAKING THE LION'S SHARE OF THE INVESTMENT MARKET

From the $30bn highs of 2021 and 2022, venture capital investment into crypto start-ups crashed in 2023 – it's on track for only $10bn, according to PitchBook data cited in the Financial Times. Of course, VC investment is generally in a slump. PitchBook's data shows venture deal volume has fallen every quarter since Q2 2022, although the lag in known deals may mean the picture isn't quite as gloomy. Either way, venture capital investment elsewhere hasn't mimicked crypto's 70% decline. On one reading, it's not so much that crypto's lost its shine but that generative AI's star is shining brighter than blockchain's ever was. In a market where there's less money around, generative AI is taking the lion's share.

Yet 2023's generative AI investment landscape has been dominated by mega-deals: Microsoft's $10bn in ChatGPT creator Open AI in Q1 and Amazon's $4bn in Anthropic, who have developed ChatGPT competitor 'Claude', according to Pitchbook data. That same data suggests that without the investments from Amazon and Microsoft, this year's overall deal value in blockchain and generative AI aren't altogether that different.

There are still plenty of VCs who are publicly backing investment in crypto, but perhaps the emphasis has changed: less about new NFT collections or decentralised cryptoasset trading, and more about tokenisation of assets.

"From $30bn highs, crypto start-up VC falls to $10bn in 2023. Generative AI steals the show, scoring mega-deals while blockchain lags behind."

MDRˣ

3

Key Sectors

In this section, we look at the key sectors that saw the most activity in 2023, and predict the key sectors to watch in the year to come.

Retail

We saw two distinct types of blockchain adoption in the retail sector through 2023: consumer-facing marketing activations; and back-office efficiency projects.

MARKETING ACTIVATIONS

From a marketing perspective, the highest-profile 2023 example is no doubt Starbucks' NFT-powered Odyssey loyalty scheme. The value proposition isn't entirely obvious. The special functionality that blockchain offers is the ability for consumers to sell on their loyalty rewards rather than use them themselves, but this raises a couple of questions. Firstly, how good would those rewards need to be for them to be worth the hassle of selling on?! Second, when loyalty points can be bought and sold, it somewhat undermines the value of the word loyalty and the purpose of the scheme. The very Web 3.0 purist dream of fully interoperable so-called "coopetition" does carry with it a fundamental tension: while consumers would not doubt enjoy and benefit from it, the notion of rewarding consumers for shopping around is contrary to the underlying business model of many brands especially those at the luxury end of the market.

"Retail's blockchain adoption: split between flashy marketing and back-office efficiency."

Selfridges has invested time and energy at an executive level to define a clear Web 3.0 strategy.

MDRx

Many retailers however know that they have to offer new, engaging, and innovative experiences to maintain their service offering. Selfridges' mission for example is to Reinvent Retail while enabling its customers to Live Brighter – it is no coincidence that it has invested time and energy at an executive level to define a clear Web 3.0 strategy, together with pursuing thoughtful and rewarding builds.

BACK-OFFICE EFFICIENCY

We are also seeing a resurgence of interest in back-office implementations of blockchain across the retail sector, including in the supply chains. This makes sense: supply chains are complex and involve often huge numbers of counterparties, while changes of state across the supply chain often need to be tracked and shared between retailers and their suppliers. Each party has information that only it can know at the time, so must share that information with all the other parties that need to know. Non-blockchain technology can, and is, being used but if every party wants reliable access to a real-time record of what everyone else in the chain is doing and the ability to automate payment triggers amongst other things, then blockchain provides a credible alternative.

There is relative academic interest in this area: a 2023 review identified more than 50 papers published between 2016 and 2021 on blockchain adoption in the food supply chain alone, but the number of new papers has dropped significantly since reaching a peak in 2019. Live implementations, however, are more difficult to come by with the IBM/Maersk TradeLens failure having a chilling effect on would-be adopters.

There are three fundamental issues to overcome in any supply chain implementation: first, blockchain is a team sport and relies on coordinating a large number of counterparties with divergent interests; second, by automating things like payment triggers we prevent certain actors (typically the big ones) from perpetually paying late and benefiting from strong cashflows; and third, the challenge of executing any digital transformation, especially without readily available off-the-shelf products that integrate with existing systems, is often too great for smaller players.

Those who have worked in the industry long enough will remember supply chains being touted as exceptional blockchain use cases twice before: once in 2015 and again in 2019-2020. The difference this time, encouragingly, is that in 2023 the majority of activity is taking place on public chains like Ethereum rather than closed so-called enterprise blockchains like Hyperledger Fabric or Corda Enterprise. This is in part a reflection of the industry's

MDRx

recognition that totally private and permissioned implementations undermine the core value proposition of distributed systems. It is also a reflection of the growing trust in the integrity and security of some of the leading public chains and the benefits of a public ledger even where the subject matter remains private.

Gaming

Blockchain gaming's distinctive features derive from the blockchain-enabled functionality of their in-game assets and the use of cryptocurrencies to pay – and get paid.

In-game assets, like characters and items, have associated NFTs that can be bought and sold quasi-independently from their parent games, connecting in-game assets to the wider NFT marketplace. Game developers could theoretically introduce buying and selling functionality without blockchain technology, but they wouldn't be able to take advantage of the existing technical and economic infrastructure of NFT marketplaces, which has no real non-blockchain analogue. The London Stock Exchange will not help you sell your Pokémon (yet).

You might question why anyone would want to buy someone else's video game character. Perhaps, for games that are sufficiently popular – or likely to become very popular – a much bigger marketplace than just players might be interested in having a stake. Video game characters with desirable characteristics that improve player performance might be valuable to a lot of people, making them an asset worth owning even if you don't play.

Are games popular enough – and assets useful enough in gameplay – to warrant a separate trading market? The most popular blockchain games only manage a count of daily unique active wallets of a bit above a hundred thousand. Many blockchain games require users to have 'wallets' to play but don't necessarily track user numbers separately; however, they're roughly comparable. A hundred thousand players is nothing to sniff at but a rounding error to the most played non-blockchain games that draw tens of millions each day. Without that kind of penetration, it's hard to see a rational market for game asset trading beyond actual players.

So perhaps the long-term success of blockchain gaming, at least for its unique asset trading features, depends on game publishers who can bring in tens of millions of players. Earlier in the year, Ubisoft, publisher of successful franchises like 'Assassin's Creed', announced its first Web 3.0 game was in development. Square Enix, creators of the 180 million copy-selling

> **"Blockchain gaming introduces tradeable in-game assets, bridging gameplay to wider markets."**

MDRˣ

Square Enix launched the website for their Web 3.0 game 'Symbiogenesis'.

Final Fantasy video game series, finally launched the website for their Web 3.0 game 'Symbiogenesis'. The company is running competitions for prospective players to create, and potentially win, playable characters in November, with the release of the game itself to follow.

In our Brand Watch, we have already covered Nike's partnership with EA Sports, publisher of FIFA, the world's best-selling sports video game. Fashion brands have been partnering with video game publishers for decades as more people have spent more and more time playing. The idea that players will enjoy greater status because their character is nicely kitted out isn't that much of a conceptual leap. Just as it's not that hard to believe that a guarantee that apparel is unique not just within one game, but every video game in existence, is something people would pay for.

There is a side to all of this that might be called a philosophy. Historically, the only ownership rights buying a game gets you is the ability to play it. Blockchain technology provides the infrastructure for a broader conception of ownership. Players can monetise the time they've invested in levelling up their characters. Players can even loan out their characters to those who don't have the time to train, or can't afford to buy, higher-level ones. Because who doesn't want to spend a magical day as a level 1000 wizard with Tiffany earrings and a Gucci cloak?

Fashion

The fashion industry is no stranger to blockchain. MDRx has supported some of the world's most prestigious fashion houses since their earliest forays into the blockchain market, and by the end of 2022, many household

Gucci released a 21 NFT collection in collaboration with Christie's and announced its collaboration with Yuga Labs.

names had launched their first collections. This year has seen much less activity, although Gucci has built on its early lead with 21 NFT collection in collaboration with Christie's, as well as an announcement of its collaboration with Yuga Labs, creators of the multi-million pound Bored Ape Yacht Club NFTs.

NFT auctions can take place entirely digitally, and the art itself can be completely digital as well. It draws on a set of technologies quite distinct from blockchain, to form experiences which MDRx describes as the Metaverse. Christie's virtual gallery allows prospective collectors to choose an avatar and roam virtual gallery spaces. At this stage, the experience is limited and does not match the production value of the most visually arresting video games. Long-term success for Web 3.0 in this area is likely to be driven by hardware developments, and improvements to premium virtual and augmented reality technologies, rather than developments in blockchain itself.

Our two sectors to watch in 2024:

Real estate

Yes, we have been here before. Tokenised real estate has reared its head as a blockchain use case for years, and the opportunity to bring accessibility and liquidity to the massive real estate investment market has captured many imaginations.

To date, most implementations have failed either because the products lack well-researched design and best-in-class execution, or because the implementations lack the assets (i.e. the real estate) required to make them worthwhile. The turbulent regulatory environment has certainly not helped either.

We are backing all of these things to change in the next 12 months. The blockchain industry has (somewhat belatedly) woken up to realise that users care about and will spend money on benefits rather than technology, the regulatory environment finally has clarity, and established incumbents are getting more comfortable with a technology that is better proven and tested.

"Tokenised real estate: tech advances, clearer regulations, and industry expertise signal a turning point in 2024."

MDRx

MDRx has a good pedigree in this sector. In 2019, for HM Land Registry, we developed a proof of concept for the transfer of the property in 10 minutes, rather than the months it would normally take. We also work closely with our Real Estate colleagues from across The MDR Group to bring industry know-how and compliance by design to our builds.

Sports

Leading teams and clubs are increasingly realising that they are not just sports teams, but rather are large rights holders and media companies. This transition has been gradual but critical.

We have been really critical of many teams who have, for too long, licensed their rights to the highest bidder. This makes some commercial sense in the short-term, but the long-term opportunity is much more profound and is too core to the overall organisation's future to be blithely outsourced forever.

With viewing and playing numbers dwindling across almost all major sports, blockchain can be one tool in the arsenal to engage fans in new and novel ways. This has been really well showcased by Veloce, the world's largest motorsports and media group, which has introduced online proposals where fans can vote on decisions that the company makes. From humble beginnings, for example, the colour on some of their sponsored race cars, the opportunity will be to make business-critical decisions that will steer the company's success from race entries to driver signings to game integrations and prize money distributions. The proposals are blockchain-based and radically transparent, while providing a viable secondary market for voting rights by interested stakeholders.

There is no shortage of creative thinking about how sports organisations could go even further. Thanks to advances in blockchain technology, it's increasingly possible to pre-program transactions based on pre-defined triggers. This opens possibilities where fans could control the flow of funds to sports organisations based on their votes. Nothing says ownership like controlling the money.

"Sports teams as media giants: a shift in strategy. Blockchain fuels fan engagement, offering transparency and a new level of fan control in major decisions."

MDRx

4

Crypto Markets

It is difficult to meaningfully discuss blockchain without at least touching on the crypto markets. In this section, we look at a few of the key metrics MDRx uses to analyse and understand the health of the ecosystem from time to time.

Market Cap, Dominance and TVL

The market capitalisation of crypto projects has gradually increased through 2023, including a very strong Q4 as of November 2023.

Market cap over 2023. Source: CoinMarketCap

It is funny that in the world of crypto, this chart looks relatively flat and stable, despite the y axis telling us that we are seeing close to a 100% YTD swing. It is however a much healthier-looking graph than its 2022 equivalent, which was a very sobering decline.

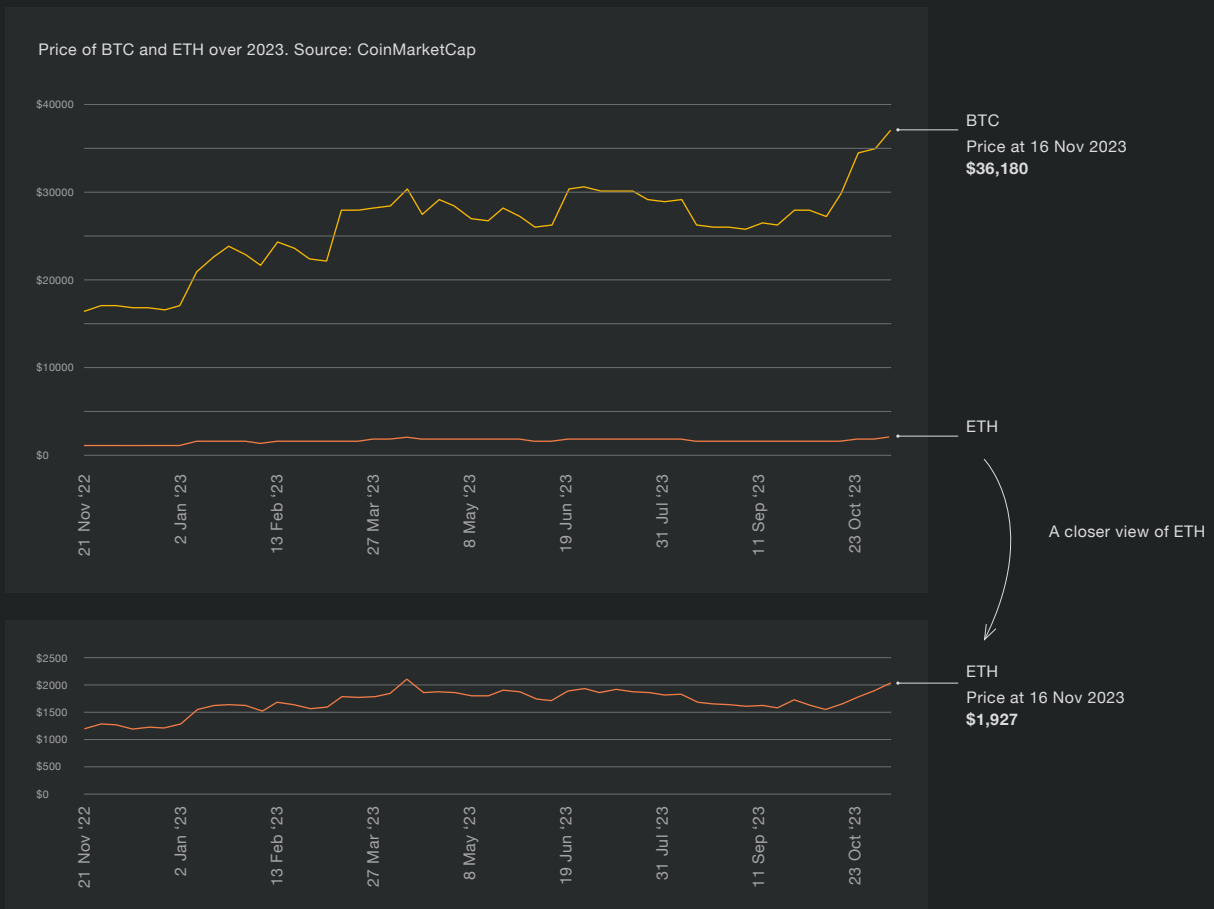Bitcoin's (BTC) dominance, and Ethereum's (ETH) position as the second-most dominant asset, remain undisputed. The slight erosion over time is consistent with what we have seen in other strong markets, while in so-called bear (we call them 'rational') markets, BTC tends to reassert itself across the market as the de-facto 'digital gold'.

Bitcoin dominance over 2023. Source: CoinMarketCap
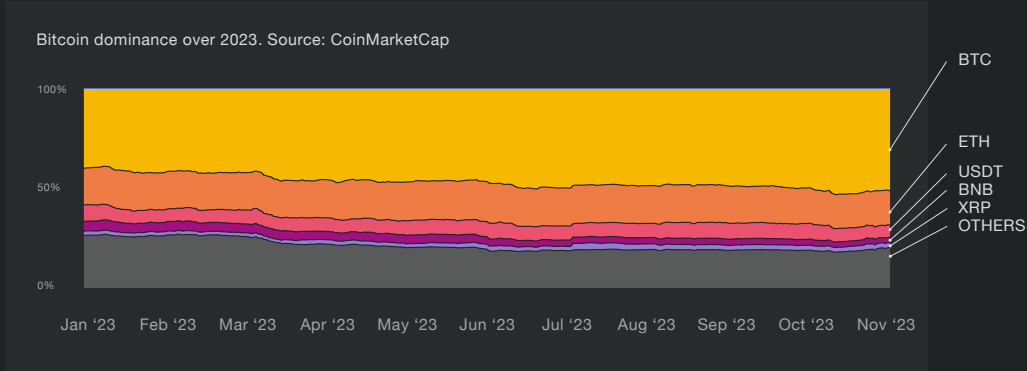
The price of BTC and ETH continues to show relative correlation, albeit ETH enjoys and endures higher velocity climbs and falls.

Price of BTC and ETH over 2023. Source: CoinMarketCap

BTC
Price at 16 Nov 2023
$36,180

ETH

A closer view of ETH

ETH
Price at 16 Nov 2023
$1,927

It is sometimes easy to forget that the journey these two assets have been on over the last 15 years is undeniably remarkable, and that a year-end position of c.$37K would have been unthinkable even five years ago.

BTC and ETH price history. Source: CoinMarketCap

A closer view of ETH
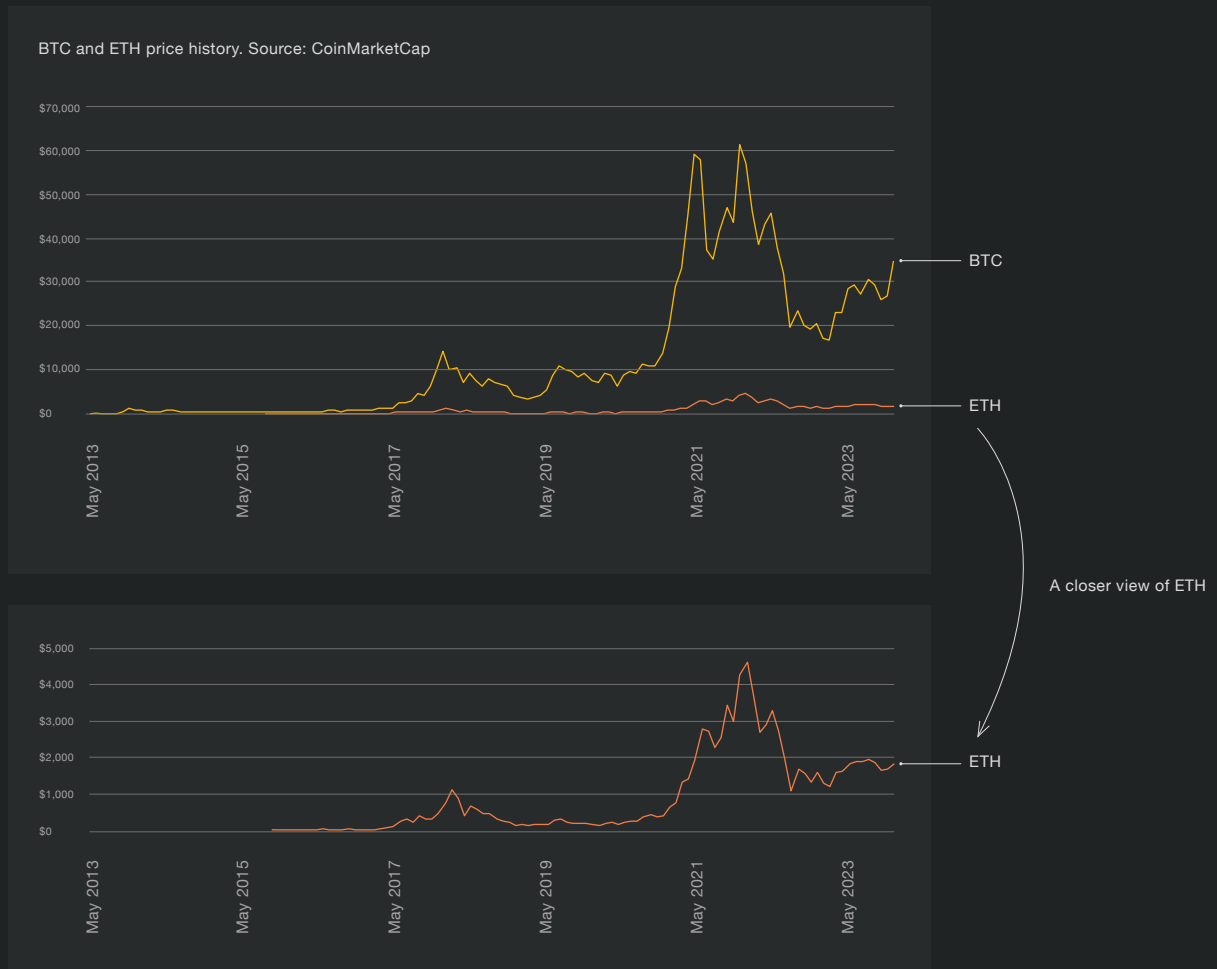
We can observe volume slightly dipping over the course of the year. There could be many factors unpinning this, from macroeconomic and cost of living to the withdrawal from key markets of some leading exchanges in response to geopolitical and regulatory developments.

All coins volume over 2023. Source: CoinMarketCap
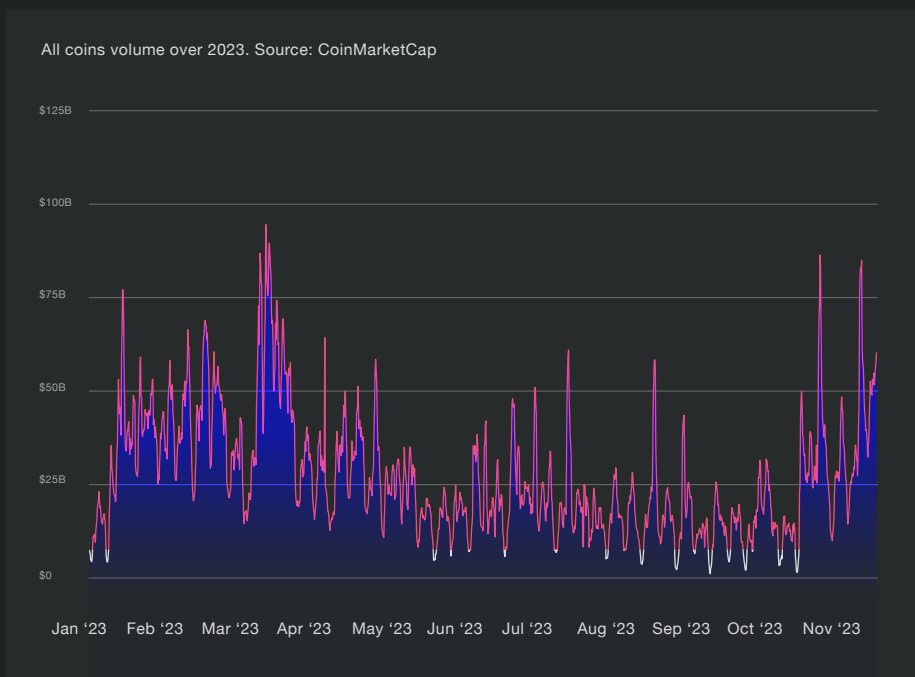
DeFi

Total value locked (TVL) is an interesting metric to assess. Excluding cryptoassets staked in decentralised autonomous organisations (DAOs), yield farming protocols and liquidity staking, as at 16th November 2023 the current composition of TVL is:

- Lending protocols account for approx. 49% of TVL
- Collateralised debt protocols - approx. 22%
- Decentralised exchanges - approx. 20%
- Derivatives - 4%
- Bridges – 1.3%
- Payments - 0.5%

We can somewhat crudely break the DeFi market down into (1) lending and collateralised lending and (2) payments.

LENDING

	Proportion of lending market & CDP market ($26.5 bn)	Y-O-Y trend on TVL	Developer activity in the last year
Aave	22%	6% growth from $5.4bn to $5.75bn	>5000 commits
JustLend	22%	77% growth from $3.6bn to $5.83bn	20 commits
MakerDAO	20%	29% decline from $7.5bn to $5.36bn	>9600 commits
Compound Finance	8%	3% decline from $2.32bn to $2.24bn	>2200 commits
Curve Finance	8%	67% decline from $6.03bn to $2bn	>2000 commits

Y-O-Y trend on TVL
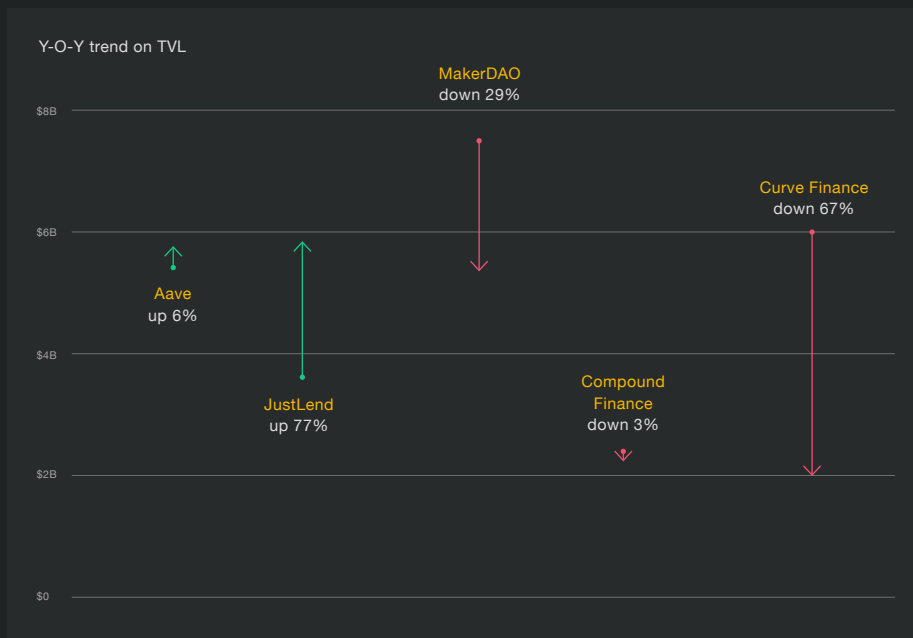
There have been several developments in this space over the last year. Aave remains a market leader, and its V3 surpassed its V2 in TVL in September 2023. Maker launched the Spark Protocol to drive DAI adoption, and Compound V3 went live on Arbitrum. The general trend of on-chain loan apps is down.

PAYMENTS

Clearly, payments remain a core value proposition for blockchain.
Key assets include:

• USDC, a stablecoin backed by Circle

• USDT, a stablecoin used on the Tron Network

• DAI, a decentralised collateralised stablecoin

• XLM, a payments and exchange network

• XRP, a payments and real-time gross settlement system

	Avg Mcap (billion)	Avg traded volume (billion)	Volume/ Mcap	Mcap	Growth or decline
USDC	24	6	25%	47%	↓ Decline
USDT	87	50	57%	28%	↑ Growth
DAI	5.35	0.19	4%	18%	↓ Decline
Ripple (XRP)	34	2	6%	74%	↑ Growth
Stellar (XLM)	3.3	0.11	3%	13%	↑ Growth

	TVL	Avg traded volume (billion)	Liquidity utilisation (traded vol/TVL)	TVL (Y-O-Y)	Growth or decline
Lightning Network	0.192	0.0005	0.26%	0.04	↓ Decline

It has definitely been a choppy and mixed year for payment stablecoins. USDC briefly broke its peg in March 2023 owing to the Silicon Valley Bank collapse, while it also expanded to other popular chains. USDT grew significantly and also released a gold-backed alternative. Stellar launched a smart contract platform called Soroban programmable in Rust. Ripple came out the marginal victor in its latest round of legal wrangling with the SEC.

MDRx

5

Spotlight: Account Abstraction

In this section, we look at an unglamorous but fundamentally important development relating to the underlying infrastructure associated with blockchain technology that has caught our attention in 2023.

Account Abstraction

The user experience using blockchain continues to carry significant friction. Account abstraction presents an important tool to smooth this out, by providing users with a mechanism to programme more security and better user experiences into their accounts for example by enabling externally owned accounts to be controlled by smart contracts, and by upgrading smart contracts to initiate transactions themselves. This smooths user experiences by reducing the need for manual individual signing and the need to maintain sufficient gas in a given wallet.

HOW ACCOUNT ABSTRACTION WORKS
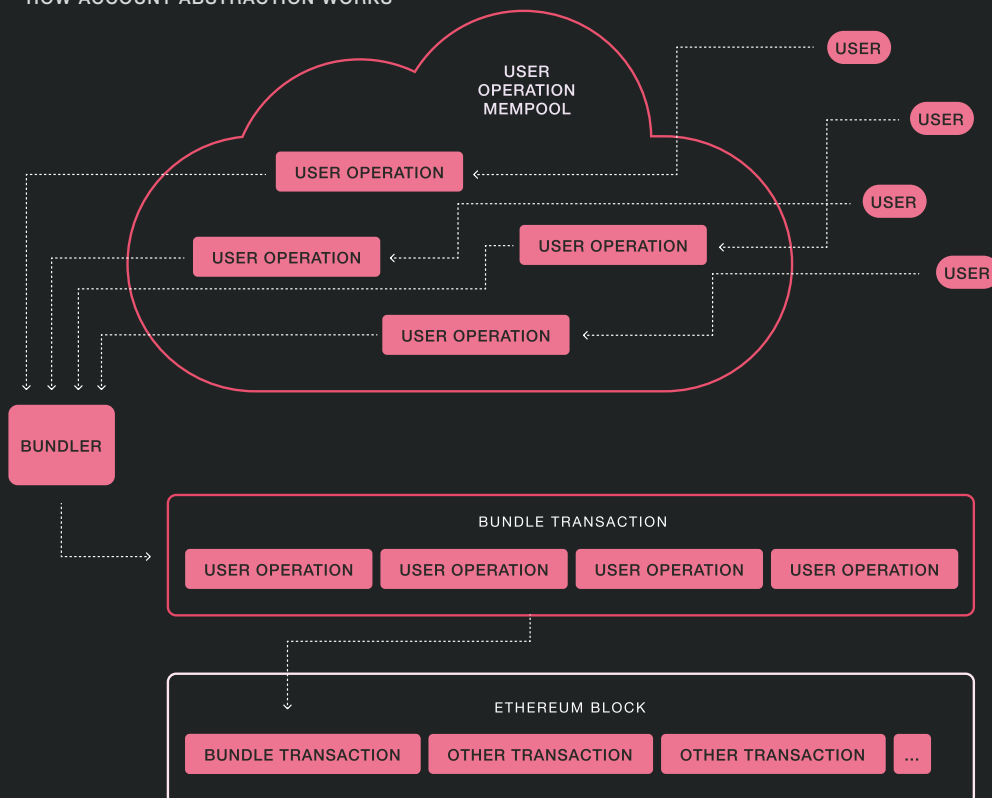
Source: Medium

The ERC-4337 standard was published in 2023, as a means of achieving the account abstraction features without needing to make changes to the underlying Ethereum blockchain. It provides a mechanism to customise validation logic, with state changes and requests being made using a special type of transaction called UserOps, which is directed to a specific memory pool (mempool) of pending and unconfirmed transactions.

UserOps relies on third-party providers known as bundlers and paymasters to bundle their requests and make payments on their behalf while validating request logic. There is of course a natural tension here between the fully disintermediated ideological dream put forth by the blockchain community, and the need to provide seamless and easy UX to onboard a billion users. We are betting that ease of access and use will win the day.

6

Barriers to Adoption

The blockchain industry has made tremendous progress over the last 15 years but there remains much to do if it is to achieve the widespread mainstream adoption it still craves. This section gives an overview of some of the key barriers to adoption as we see it.

Use-cases

We have ended every year for the last decade bemoaning the absence of the "killer app". The industry took far too long to grasp that mainstream audiences do not care at all about technology, barely care about features, and only really care about the benefits and experiences offered by new innovations. Still, most of the blockchain industry exposes far too much tech-speak to its users which serves only to confuse, overwhelm, and alienate them.
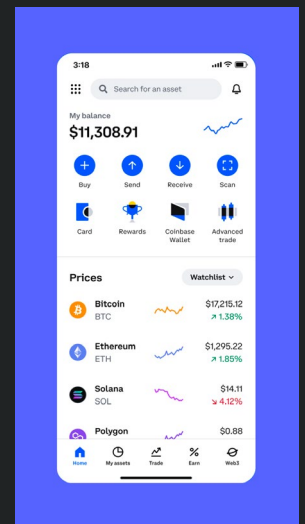
Contrast this position with the recent rise of generative AI. ChatGPT did not acquire 100m users in such a short time because they all fell deeply in love with the underlying data model or formed a fundamental appreciation of the transformer's pre-training. It did so by putting an easy-to-use tool in the hands of consumers, that could generate useful, interesting, sometimes weird outputs.

Once Web 3.0 products can deliver a user experience that significantly abstracts away the underlying tech while also delivering a key need in a way that is both easy to engage, and easy to use, the hurdles to adoption will be diminished. We have earmarked some of the key sectors to watch in Section 3 above.

Coinbase is an example of an app for buying, selling and trading crypto

Regulation

The view that regulation and innovation are diametrically opposed is overly simplistic and, in many cases, flawed. Indeed, history gives us many examples whereby innovation was turbocharged by regulatory intervention, from the EU's regulation of e-commerce in the early noughties to Gibraltar's pioneering online gambling regime.

The true innovation killer is legal and regulatory uncertainty, which has existed for far too long with respect to blockchain and other distributed ledger technologies. This year, excitingly, the position in England and Wales is onerous but it has a new level of certainty that we welcome. The application of the new financial promotions regime in the UK, which bites

on anyone marketing into the UK irrespective of the jurisdiction in which they are incorporated, also renders many complex (and expensive) off-shore structures valueless.

Would-be adopters of blockchain now have a clear choice:

1. commit to compliance by design and launch their product in or into the UK; or

2. withdraw from the UK market entirely, or else risk the wrath of the FCA.

MDRx exists to help businesses that want to explore option 1, and deliver incredible, innovative, and responsible results. We probably aren't for you if option 2 appeals.

Coordination

Decentralisation is a feature, not a bug, of blockchain. It does however make it challenging to produce industry-wide consensus and change. It also limits the ability for proper advocacy, with disproportionate weight given to the centralised actors in the ecosystem with large lobbying budgets.

The Ethereum Foundation's stewardship stands out in this respect, and the engineering feat required to pull off The Merge and other upgrades is truly impressive. It is rather centralised in its approach however, and the inability to convene enough consensus to amend Bitcoin stands in stark contrast (though of course, Bitcoin maximalists will argue that this too is a feature and not a bug).

There is no silver bullet for this challenge, but it is helpful to reflect on it and therefore temper our predictions on how quickly things might move in the future.

User experience

It's still horrible. It's way better than it was. But it's still horrible. We are encouraged by the great infrastructure work being done to smooth the process and make engaging with blockchain applications a delight, and we also believe that the regulatory certainty afforded in England and Wales now

will encourage large actors to enter the ecosystem with greater confidence, bringing with them world-class engineering at a scale to properly move the needle and improve UX for all.

Brand

There perhaps is no more divisive technology than blockchain. Most of the rhetoric on both sides is bizarrely tribal, attracting the sort of binary thinking that tends to veer into idiocy. It's fair to say however that the blockchain industry really doesn't help itself...

We need grown-up and transparent organisations, inspiring and responsible leaders, and a community that unflinchingly holds them to account rather than acting as either cheerleaders, apologists or vigilantes. MDRx is really proud of the clients we act for in this space and believes in their commitment to uphold these values. If we did not, we wouldn't work for them.

7

Look Ahead 2024

This section contains our predictions for the year to come.

Terminology

The terms 'crypto', 'blockchain', and 'Web 3.0' are polarising at best. The most interesting projects coming to us now are not mentioning any of these terms, and instead are focused on features and user benefits, while the technologies used to provide them are rightly irrelevant in their marketing materials. We expect to see this trend continue from major brands in 2024.

Increasing regulation

Regulatory scrutiny is expected to intensify. Many jurisdictions will follow the lead of England and Wales in expanding their regulatory perimeters to encompass all cryptoasset projects marketed within their borders, regardless of where these projects are incorporated and operated from. We expect this will critically undermine and lead to the unwinding of some very expensive offshore structures used to conduct regulatory arbitrage through 2024.

Industry-wide regulation is not only inevitable but also beneficial. If blockchain is to onboard a billion users, it must have some protections. This goes against the blockchain purist sentiment that on-chain activity should be elevated above legal and regulatory enforcement, but we don't hold much stock in this viewpoint.

There is a significant possibility that the UK's current FCA regulations serve as a blueprint for governments in Africa, Asia, and the Middle East. These

regions may adopt similar frameworks to establish industry standards and ensure the safety of their citizens while jostling for global market share.

Legal actions and prosecutions

We think more people will go to jail.

There are way too many bad actors in the space, and it will be to the industry's benefit to take some high-profile scalps. The public blockchain ecosystem will not gain mass and institutional buy-in if it remains controlled by exchanges acting like corrupt banks with murky market-making activity and opaque treatment of customer funds.

Targeted, activist private litigation will have a huge part to play alongside regulatory actions and prosecutions. May it bring long overdue sanity to the industry.

Tokenisation

Tokenisation will be big in 2024. After a few quiet years, we are expecting to see the tokenisation of financial markets continue (looking at you, JP Morgan, BlackRock and Barclays) as well as other major asset classes including real estate.
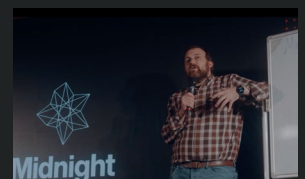
We last saw this trend in 2018, and since then we have wider industry acceptance, better infrastructure, and an onerous but ultimately clear and permissive legal and regulatory framework. Expect to see several projects launch, many fail for lack of adoption, but some come good and thrive.

Cross-chain protocols

Interoperability has been a blockchain dream since 2016. There is no predestined winner apparent yet, but whoever emerges will have a hugely important, valuable, and profitable role to play in the market. We have our eyes on several projects, including Chainlink's CCIP, Quant, LayerZero, Axelar and Celer Network. Their contributions will be pivotal in shaping the interoperability landscape.

Charles Hoskinson, co-founder of the blockchain engineering company IOHK (Input Output Hong Kong Source: youtube.com/ @midnight.network

Compliance by design

It is no longer optional for responsible organisations to bake compliance into every phase of their product strategy and engineering. Together with many compliance-friendly and off-the-shelf tools in the market like IOHK's Midnight, MDRx is here to make that happen.

Appendix

In case it's helpful: A Blockchain refresher

Part A: Blockchain, cryptoassets and the evolution of ledgers

Blockchain is a subset of distributed ledger technologies (DLT), being a group of technologies that use different techniques and structures to store, synchronise and maintain a shared ledger of digital records across a network of computing centres. Many types of DLT are not technically structured as blockchains, but for this report, we use the terms blockchain and DLT interchangeably unless specifically stated otherwise.

THE EVOLUTION OF LEDGERS

A ledger is a book or collection of accounts in which accounting transactions are recorded. The idea of maintaining a ledger is not a new one. The earliest ledgers date back to c.4,000 BC in Mesopotamia. These ledgers were kept on clay scripts or carved into stone, and were used to record and demonstrate definitive ownership, and the transfer of ownership, of crops in storage. Recording the ownership and movement of value has been a central tenet of human civilisation ever since. The form and structure of these ledgers however has evolved (and continues to evolve) with time.

The Mesopotamian example describes what we now call a centralised ledger (see Fig 1 below), in which a single definitive ledger exists within an ecosystem. In many circumstances, such centralised ledgers are effective, and many remain in use today – for example, a registration in a school. Centralised ledgers do however have some drawbacks, notably that they have a single point of failure (i.e. the single ledger). If the ledger is lost, stolen or attacked (i.e. tampered with by a third party), the ecosystem and its participants (those placing reliance on the definitive nature of the ledger's record keeping) will fail. As an ecosystem becomes more complex and its value rises, the use of a centralised ledger becomes less appropriate.

As civilisation has developed, so too have decentralised ledgers become more prevalent (see Fig 1). In modern society, we often rely on trusted intermediaries to keep and maintain common ledgers. These intermediaries may for example be financial institutions, which keep and maintain ledgers relating to our finances. Decentralised ledgers, just like their centralised cousins, are widely used today but also have their own drawbacks. They too have points of failure which can have a widespread impact on the wider ecosystem – see for example the damage caused when a financial service provider's IT infrastructure suffers an outage. They also rely heavily on the trustworthiness and integrity of the intermediary maintaining the

decentralised ledger – if this intermediary causes loss to its stakeholders through negligence or fraud, those stakeholders often have limited recourse.

BLOCKCHAINS

Distributed ledgers such as blockchains seek to avoid the drawbacks associated with centralised and decentralised ledgers by, amongst other things, removing points of failure (see Fig 1). Blockchains involve the ledger (or parts of the ledger) being replicated and stored across a network of computing centres. This network of computing centres, known as nodes, works to update the ledger as new updates (i.e. transactions) arise, and propagate the updated ledger to the network. Blockchains are, theoretically, infinitely scalable, and by distributing their control and maintenance, seek to mitigate against the risk of attack.

Figure 1: Centralised, decentralised, and distributed ledgers. Note that the structures of these ledgers, in particular the distributed ledger, have been simplified for illustrative purposes.

CENTRALISED   DECENTRALISED   DISTRIBUTED

CRYPTOASSETS AND WALLETS

In this report, we use the term cryptoassets loosely to mean an asset that is represented digitally on a DLT platform. Such assets might exist purely digitally, for example, a so-called cryptocurrency such as Bitcoin (BTC), or physically, for example, a piece of real estate that is represented by way of tokenisation.

We also refer to wallets. Again, we use this term broadly to mean the digital device used to store a user's public and private keys, which are used to manage and control the user's DLT-stored records and/or cryptoassets. Please see Fig 2 below for details regarding the purpose and functionality of public and private keys in the context of DLT systems.

Part B: Main features of blockchain

A series of mechanisms and computer protocols dictate how blockchains work – namely, how their network participants may create, amend and synchronise records held on them. These mechanisms and computer protocols typically seek to:

1. enable network participants to exclusively control 'their' records or cryptoassets;

2. maintain a clear chronology of distributed ledger entries; and

3. provide a mechanism by which nodes reach a consensus, thereby ensuring a common, synchronised ledger.

These three components represent key features of DLT. Each of them is explored below in more detail.

I. EXCLUSIVITY

To enable network participants to exclusively control their cryptoassets, most DLT implementations utilise public key cryptography.

Public key cryptography is a cryptographic system that uses two types of information (typically a fixed-length string) known as keys:

• **public keys:** these may be widely disseminated and known to some or all other network participants; and

• **private keys:** these should be known only to the relevant network participant.

If a network participant wishes to broadcast a ledger entry (for example in the case of cryptoassets, make a transaction), they would:
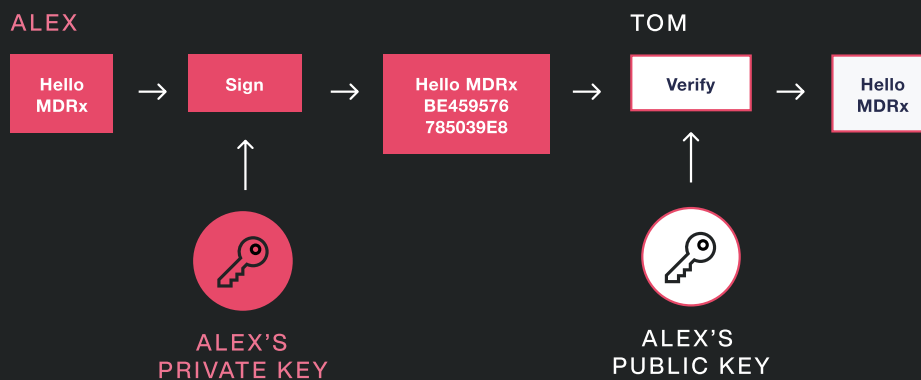
1. enter their ledger entry together with the intended recipient's public key (or a hash of the intended recipient's public key, known as a wallet address); and

2. sign the message (or transaction) using their private key.

The wider network is then able to verify that the ledger entry is genuine, by entering the public key of the network participant who broadcasted the ledger entry.

MDRˣ

When combined, the ledger entry will (provided the public key entered is indeed associated with the private key used to broadcast the ledger entry) be decrypted.

Public key cryptography is also known as asymmetrical cryptography. This is because a ledger entry encrypted using the sender's private key can be decrypted using the sender's public key, without revealing or compromising the security of the sender's private key.

Figure 2: Public key or asymmetrical cryptography-enabled messaging

ALEX

| Hello MDRx | → | Sign | → | Hello MDRx BE459576 785039E8 | → | Verify | → | Hello MDRx |

ALEX'S PRIVATE KEY

TOM

ALEX'S PUBLIC KEY

An important conceptual point to grasp is that wallets do not contain records or cryptoassets. All that is contained in a wallet is a private key. Accordingly, when we broadcast a new ledger entry on a blockchain we do not 'send' records or cryptoassets per se, rather we broadcast a ledger entry (for example a debit and credit notice) to the network's nodes, which then update their respective copies of the ledger accordingly.

Blockchain therefore enables exclusive ownership of records and cryptoassets by ensuring that the right to broadcast transactions on behalf of a public key relies on a private key, which is capable of being kept secret and known only to a single individual. In this way, an individual can be said to 'own' (albeit indirectly) certain cryptoassets.

II. CHRONOLOGY

One of the main challenges that faces a distributed ledger is how to establish a clear chronology of records or transactions. As the network becomes larger and more distributed across territories and time zones, so the 'Distributed Ledger Problem' becomes more pronounced.

The Distributed Ledger Problem

Records and transactions are passed from node to node within the network, and therefore the order in which transactions reach each node can differ.

For example, say an attacker has a wallet holding 1 MDRx Coin (a fictional cryptoasset used for illustrative purposes only). Exploiting the Distributed Ledger Problem, the attacker may make a purchase from a supplier of goods and send 1 MDRx Coin to the supplier as payment. The attacker would then wait for confirmation that the supplier had shipped the goods. Once the attacker has received the confirmation, he or she would then send a transaction to another of his wallets for 1 MDRx Coin. Due to the Distributed Ledger Problem, some nodes might receive the second transaction before the first. Those nodes would then consider the initial transaction invalid, as the transaction inputs would be marked as already spent.

If sufficient nodes to satisfy the distributed ledger's consensus protocol believed the second transaction to be the 'true' transaction, the transfer of MDRx Coin to the supplier would be rejected and the supplier, having already shipped the goods, would be out of pocket.

III. CONSENSUS

Each DLT node has its own view of the state of the distributed ledger at a given time. The result of this, exacerbated by the Distributed Ledger Problem set out above, is that, at any one time, there may be as many views of the present state of the ledger as there are nodes in the network.

Distributed ledgers implement clear rules to enable their constituent nodes to reconcile differences and record messages and transactions in a harmonious fashion. These rules are known as consensus protocols. There are a number of 'flavours' of consensus protocols, each with its own trade-offs that in turn impact the distributed ledger's performance and functionality. See below for some high-level examples of consensus protocols.

Part C: Consensus protocols

DLTs may leverage a range of different consensus protocols. The following is a high-level overview of two well-known examples: proof of work and proof of stake.

I. PROOF OF WORK

Proof of work requires participating nodes (known as 'miners') to prove that computational resource (i.e. effort by a node) has been committed before a record of transactions can be accepted as part of the distributed ledger. Proof of work is perhaps the best-known example of a consensus protocol and is used by the Bitcoin (BTC) blockchain.

To prove their commitment of computational resource, miners 'race' to solve a computational puzzle which is designed to require a large number of computational steps without shortcuts. Once solved, the successful miner can broadcast the answer to the puzzle to the DLT's node network, which can then easily and quickly verify the answer as being correct and thus accept the new entry to the ledger. Most DLTs require a majority of nodes to verify the puzzle answer in order to accept the entry of the new records or transactions to the ledger. Typically, in DLTs that use proof of work, mechanisms are built in to reward and incentivise miner activity.

Proof of work's advantages include that it is secure (subject to a well distributed network of computing power), it deters spam (by requiring miners to expend effort in order to successfully enter new ledger entries), and it is democratic (as the same puzzle is posed to all miners). It has however been criticised for being, amongst other things, relatively slow, expensive (owing to the hardware required to give miners a reasonable prospect of success, which undermines its democratic credentials), and environmentally unfriendly (owing to the energy consumption associated with mining activity).

II. PROOF OF STAKE

Proof of stake requires each node that seeks to update the ledger to prove that it has a 'stake' in the system. In 2022 we saw the Ethereum Foundation complete The Merge, leading to the adoption of proof of stake by the Ethereum blockchain network. Other well-known implementations of proof of stake include Stellar, DASH and NEO.

To establish a new ledger entry, competing nodes (known as 'validators') construct a particular type of transaction that 'locks-up' their funds in a form of deposit. Validators then take turns proposing and voting on the next ledger entry. The weight of each validator's vote is proportionate to the size of its lock-up. If a majority of validators reject a proposing validator's ledger entry, the proposing validator loses its lock-up.
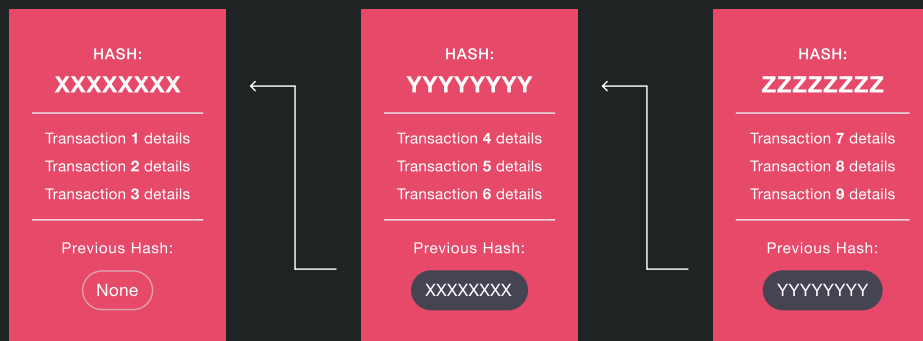
In addition to deterring validators from proposing fraudulent new entries (for fear of losing their lock-up), proof of stake DLTs also ensure that the state of their ledger is dictated by those invested in them – those investors will wish to ensure the integrity of the ledger as, if doubt is cast upon it, the value of the DLT (and in turn the investor's investment) will diminish. Other advantages of proof of stake include that it is quicker and more energy efficient than some other consensus protocols (such as proof of work). Disadvantages of proof of stake include that is more difficult to secure and can be seen as undemocratic.

Part D: Blockchain

The best-known example of a DLT is blockchain, which rose to prominence on the publication of the Bitcoin white paper in 2008 under the pseudonym Satoshi Nakamoto. Blockchains bundle digital records into data container structures known as 'blocks'. These blocks are appended to the end of a chain of blocks in chronological order, hence the name.

Typically, each block in a blockchain will contain a hash of the preceding block. This ensures that a clear, irrefutable chronology is established and maintained.

Figure 3: Blockchain structure

HASH:	HASH:	HASH:
XXXXXXXX	**YYYYYYYY**	**ZZZZZZZZ**
Transaction **1** details	Transaction **4** details	Transaction **7** details
Transaction **2** details	Transaction **5** details	Transaction **8** details
Transaction **3** details	Transaction **6** details	Transaction **9** details
Previous Hash:	Previous Hash:	Previous Hash:
None	XXXXXXXX	YYYYYYYY

MDRˣ

AUTHORS

Alex Slowman
Senior Researcher

Tari Ajienka
Blockchain Engineer

Toba Ajiboye
Blockchain Engineer

Tom Grogan
CEO

CONTRIBUTORS

Alex Shaw
CTO

Dulcie Pearson
Strategy and Product
Consultant

Narcisa Lupu
Content Marketing Manager

DESIGN

Omair Barkatulla
Amy Niven

MDRˣ

MDR^x

To discuss anything you've read
in this report in more detail, get in
touch at hello@mdrx.tech

Address:
Africa House, 70 Kingsway,
London WC2B 6AH

Phone: 020 3321 7000

https://mdrx.tech/