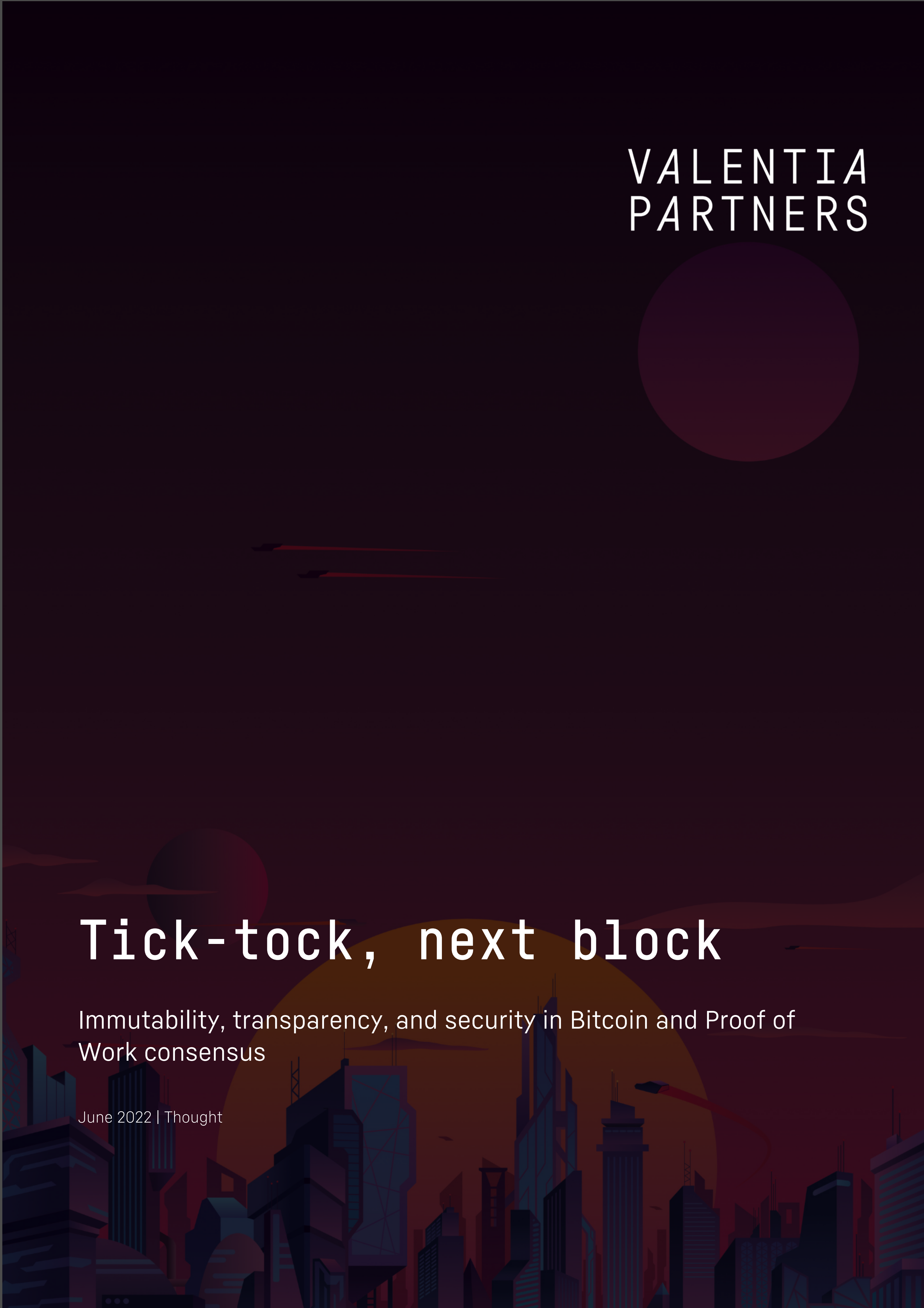
VALENTIA
PARTNERS



Tick-tock, next block

Immutability, transparency, and security in Bitcoin and Proof of Work consensus

June 2022 | Thought

Tick-tock, Next Block

In contrast to the current uncertain global macroeconomic outlook and persistent loose monetary policy, Bitcoin's immutable properties have not changed, and it continues to act precisely as it was designed when first established in 2009. This article explores key considerations for how traditional financial institutions can engage with Bitcoin's underlying technology and the proof of work consensus mechanism.

June 3rd saw members of the New York State Senate vote in favour of a bill to ban cryptocurrency mining operations that use proof-of-work consensus mechanisms due to concerns around the energy / environmental impact of mining. In March, a similar vote reached the European Parliament's economic and monetary affairs committee, which resulted in a narrow rejection by MEPs. Essentially, these can be considered votes to ban Bitcoin and, to a lesser extent, other crypto technologies that use proof-of-work.

Bitcoin (B) and bitcoin (BTC)

Bitcoin is a digital monetary network with an immutably scarce, digitally native currency – bitcoin (Bitcoin" with a capital "B" is the Bitcoin network. Bitcoin with a lower case "b" or BTC is the currency).

Holding indirect votes to ban Bitcoin, the genesis use case for blockchain technology and the most secure and decentralised cryptocurrency, while simultaneously promoting an international blockchain strategy to ensure Europe becomes a "blockchain leader and innovator", sends mixed signals across all industries.

Industry participants may, understandably, ask why some blockchain solutions are the focus of international strategies while others face regular threats of prohibition. The answer lies beneath the noise of the crypto assets; in understanding the underlying technology, the benefits, and trade-offs of different blockchains – and recognising the suitable use cases for these varying configurations.

Financial Services is undoubtedly the target sector identified for disruption, streamlining, and disintermediation by blockchain technology. This article is the first instalment of a series where we invite you to ignore the volatility of bitcoin (BTC – the underlying unit of currency) and forget about attempting to predict future price movements. Instead, we shall explore the intricacies of Bitcoin's technology (B) and its innate payments network.

Despite significant volatility in BTC (down 50% from all-time highs over a seven-month period, but still up 397% since Jan 2020[1]), reflecting investor uncertainty in valuation as an asset class, the underlying technology on which it is built has remained unchangingly consistent. It is this consistency, as a sophisticated underlying platform to underpin asset trading, that drives our interest in Bitcoin (B). Understanding and engaging with the underlying technology, and looking past surface-level commentary on BTC volatility, is critical for firms looking to future-proof for any impending industry disruptions.

In this article we introduce the critical aspects of Bitcoin at a high level, and why Financial Services players should engage with it and other select blockchain infrastructures. We compare Bitcoin's blockchain with others and engage in the broader discussion about blockchain's application (and non-application) across the Financial Services industry – from retail payments to cross-border interbank settlement, and central counterparty clearing houses (CCPs). Subsequent articles in this series will dive deeper into the underlying technology and its workings.

[1. PRICES AS OF 01/01/20 & 10/06/22]

Bitcoin (B), nodes, and proof of work

- The Bitcoin network (B) doesn't require a trusted, centralised, third party to govern it. Bitcoin (BTC) can be sent globally, settled, and custodied without any intermediary.
- Bitcoin's (BTC) supply schedule is algorithmically predetermined and cannot* be changed. There is a fixed supply of bitcoin – no matter how many miners join the network, there will never be more than 21,000,000 BTC.

This decentralised technology results in a monetary system that contrasts significantly with the current centralised global financial landscape. Bitcoin's blockchain is permissionless and decentralised. Network participants can enter freely, are responsible for validating transactions, and ensuring the integrity of the network. This feat alone should have Bitcoin on every FS executive's radar.

The integral part of enabling this decentralised process is nodes, of which there are two main types of Bitcoin nodes. It is crucial to distinguish between mining nodes (miners) and full nodes. These nodes perform separate but harmonious functions for the network:

Miners:

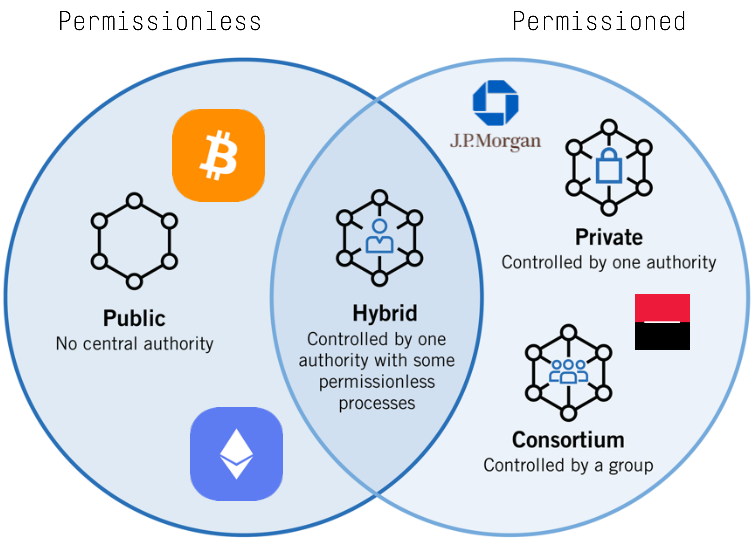
1. Confirm Transactions
2. Secure the Blockchain
3. Participate in the fair distribution of new bitcoins

Full nodes:

1. Validate Transactions
2. Keep a historic record of transactions
3. Dictate and enforce the rules of the network

Bitcoin nodes reach consensus using a Proof of Work mechanism. Put simply, this mechanism requires and incentivises network participants (miners) to expend real effort (fixed costs and energy) to prevent anybody from gaming the system. Bitcoin's incentives make it highly resistant to any changes that could alter, from a technology lens, the integrity of the assets on the blockchain. In the way we are describing assets here, we are typically referring to bitcoin (BTC), but the same principles are applicable for any proof-of-work consensus mechanism.

Exhibit 1
Types of Blockchains



This tangible effort is integral to Bitcoin's network security and decentralisation. Proof of Stake, an alternative consensus mechanism that selects validators in proportion to their quantity of holdings, makes trade-offs regarding the crucial aspects of decentralisation and tangible security. In the case of Proof of Stake, those with the largest holdings wield more power and influence. This stake can result in self-damaging effects to the network that can interfere with the overall integrity of the assets on the blockchain. For example, incentivising collusion, attacks, and perpetual centralisation – as staking rewards provide a mechanism for internal (central) parties to guarantee perpetual growth in the fraction of control they have.

Many new protocols shout about Proof of Stake's benefits but murmur its trade-offs – a discussion for a future article.

Why Proof of Work?

It is worth understanding why Bitcoin needs security and true decentralisation. In the case of Bitcoin, the goal is to establish a global payment system where anyone can participate, only the rightful owner can spend a coin, and all valid transactions eventually make it into the ledger. Quite the mission.

Network decentralisation and impenetrable security are much less relevant if you plan to use blockchain technology to "disrupt", say, the gardening industry – where the impact of a bad actor on the ledger or ledger errors is unlikely to be as significant.

Network security

- If it were profitable for miners, we would expect them to undo transactions all the time, including transactions of other people who pay them to do so.
- This would destroy the fundamentals of the distributed ledger, enabling those adequately incentivised to un-do or re-write the ledger. Because it requires energy and expensive specialised machines to mine and unlock the block reward, there is an actual cost associated with creating bitcoin (BTC).

This energy cost, that is unique to the Proof of Work mechanism for consensus, disincentivises an attack on bitcoin because the high costs of an attack are unprofitable compared to the gain if the same resources were spent on honest mining. As more miners come online and the network grows, the cost of a 51% attack (a hypothetical scenario in which more than 50% of Bitcoin's nodes / miners fall under the control of a single group) becomes increasingly unattainable and economically disincentivised.

Use cases in Traditional Finance (Tradfi)

Bitcoin's blockchain is permissionless, open and decentralised, and participants commit tangible resources to ensure it stays so. However, as we mentioned in our gardening example, these conditions are unnecessary for all use cases.

In the immediate horizon, the traditional, centralised finance model will continue to benefit more from permissioned blockchain networks than permissionless decentralisation.

- Blockchain technology can be implemented in a centralised manner, relying on centralised security and centralised validators and governors, whilst maintaining all the functionality of decentralised blockchains.
- In some areas, it may even perform better – such as transaction throughput, due to fewer nodes managing transaction verification and consensus.
- Permissioned blockchains may be less energy-intensive (albeit with a greater single point of failure and other trade-offs), but are essentially recreating traditional, centralised finance on blockchain rails.

In many of our discussions with Financial Institutions, we encounter proposed use cases where blockchain is arguably the inferior technology vs. traditional technical solutions.

Tradfi on blockchain rails is rational if that is the goal; as it is for JP Morgan's blockchain-powered repo market tool, SWIFT's recent experiments to interlink domestic CBDCs for seamless cross-border payments, or Wells Fargo and HSBC using blockchain for interbank FX settlement. These are all examples of solutions that deserve exploration in future articles.

However, the true uniqueness of Bitcoin technology remains in the purist view of digital scarcity and decentralisation – a network where participation is open, and all participants assure integrity. Proof of Work and mining are the mechanisms that underpin the decentralised clearinghouse, by which transactions are validated and cleared. Mining is the invention that makes bitcoin special.

The future:

Global demand for systems with verifiable integrity are increasing yet the path towards decentralised transparency, that dawned from 2009's genesis block, remains uncertain across financial services.

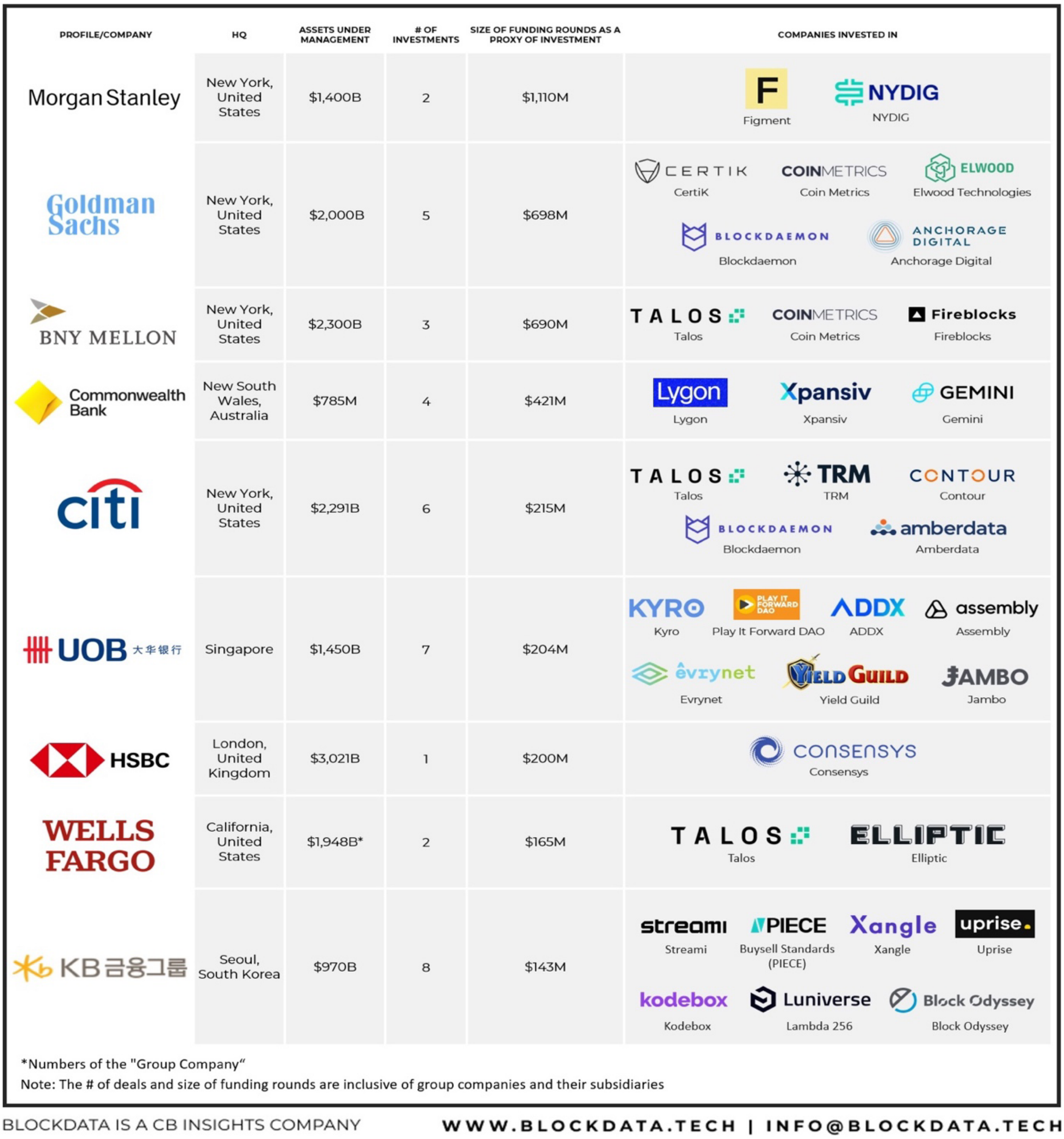
We are beginning to see a dichotomy of the opinion of governments, regulators, and international bodies regarding which blockchains are considered most appropriate to underpin global strategic initiatives. In the case of genuinely permissionless immutable blockchains like Bitcoin, the debate will intensify, regulation will evolve, and uncertainty in the general state of play looks likely to continue. The route to win in crypto innovation and capability, lies in understanding and identifying the opportunities across customer proposition, processing, and security – leveraging the unique capabilities of the underlying blockchain technology.

In the case of Bitcoin and the Proof of Work mechanism, this lies in the true immutability of the system – where integrity is enforced by all participants. When financial institutions are looking to blockchain as an enabler to build true transparency into the financial ecosystem, understanding Bitcoin's accomplishments on a technical level is critical.

Asset classes can spike and fall, central intervention / backstops in markets can waver, and traditional technology systems can fail; but throughout the Bitcoin blockchain consistently creates blocks and allows users to transact 24/7 – tick-tock, next block.

Exhibit 2

Top Banks Investing in Crypto & Blockchain Companies (August 2021 – May 2022)



PROFILE/COMPANY	HQ	ASSETS UNDER MANAGEMENT	# OF INVESTMENTS	SIZE OF FUNDING ROUNDS AS A PROXY OF INVESTMENT	COMPANIES INVESTED IN
Morgan Stanley	New York, United States	$1,400B	2	$1,110M	Figment NYDIG
Goldman Sachs	New York, United States	$2,000B	5	$698M	CertiK Coin Metrics Elwood Technologies Blockdaemon Anchorage Digital
BNY MELLON	New York, United States	$2,300B	3	$690M	Talos Coin Metrics Fireblocks
Commonwealth Bank	New South Wales, Australia	$785M	4	$421M	Lygon Xpansiv Gemini
citi	New York, United States	$2,291B	6	$215M	Talos TRM Contour Blockdaemon Amberdata
UOB 大华银行	Singapore	$1,450B	7	$204M	Kyro Play It Forward DAO ADDX Assembly Evrynet Yield Guild Jambo
HSBC	London, United Kingdom	$3,021B	1	$200M	Consensys
WELLS FARGO	California, United States	$1,948B*	2	$165M	Talos Elliptic
KB금융그룹	Seoul, South Korea	$970B	8	$143M	Streami Buysell Standards (PIECE) Xangle Uprise Kodebox Lambda 256 Block Odyssey

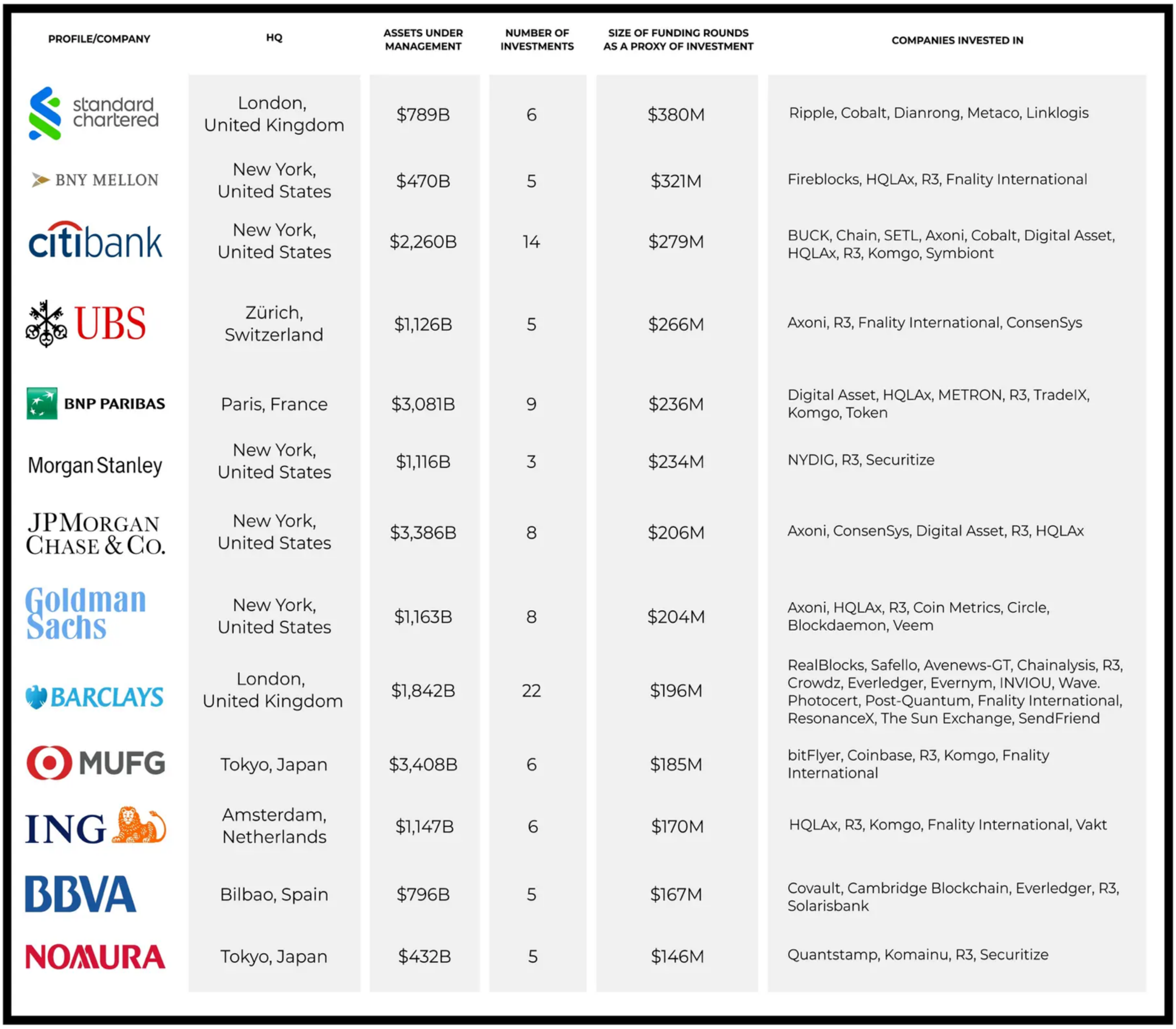
*Numbers of the "Group Company“

Note: The # of deals and size of funding rounds are inclusive of group companies and their subsidiaries

BLOCKDATA IS A CB INSIGHTS COMPANY   WWW.BLOCKDATA.TECH | INFO@BLOCKDATA.TECH

Exhibit 3

Top Banks Investing in Crypto & Blockchain Companies (August 2021)



PROFILE/COMPANY	HQ	ASSETS UNDER MANAGEMENT	NUMBER OF INVESTMENTS	SIZE OF FUNDING ROUNDS AS A PROXY OF INVESTMENT	COMPANIES INVESTED IN
standard chartered	London, United Kingdom	$789B	6	$380M	Ripple, Cobalt, Dianrong, Metaco, Linklogis
BNY MELLON	New York, United States	$470B	5	$321M	Fireblocks, HQLAx, R3, Fnality International
citibank	New York, United States	$2,260B	14	$279M	BUCK, Chain, SETL, Axoni, Cobalt, Digital Asset, HQLAx, R3, Komgo, Symbiont
UBS	Zürich, Switzerland	$1,126B	5	$266M	Axoni, R3, Fnality International, ConsenSys
BNP PARIBAS	Paris, France	$3,081B	9	$236M	Digital Asset, HQLAx, METRON, R3, TradeIX, Komgo, Token
Morgan Stanley	New York, United States	$1,116B	3	$234M	NYDIG, R3, Securitize
JPMorgan Chase & Co.	New York, United States	$3,386B	8	$206M	Axoni, ConsenSys, Digital Asset, R3, HQLAx
Goldman Sachs	New York, United States	$1,163B	8	$204M	Axoni, HQLAx, R3, Coin Metrics, Circle, Blockdaemon, Veem
BARCLAYS	London, United Kingdom	$1,842B	22	$196M	RealBlocks, Safello, Avenews-GT, Chainalysis, R3, Crowdz, Everledger, Evernym, INVIOU, Wave. Photocert, Post-Quantum, Fnality International, ResonanceX, The Sun Exchange, SendFriend
MUFG	Tokyo, Japan	$3,408B	6	$185M	bitFlyer, Coinbase, R3, Komgo, Fnality International
ING	Amsterdam, Netherlands	$1,147B	6	$170M	HQLAx, R3, Komgo, Fnality International, Vakt
BBVA	Bilbao, Spain	$796B	5	$167M	Covault, Cambridge Blockchain, Everledger, R3, Solarisbank
NOMURA	Tokyo, Japan	$432B	5	$146M	Quantstamp, Komainu, R3, Securitize

BLOCKDATA IS A CB INSIGHTS COMPANY

WWW.BLOCKDATA.TECH | INFO@BLOCKDATA.TECH

For more information contact:

Vince Giltinan | Analyst
vincent@valentiapartners.com

Recently working with a leading crypto exchange on strategy and project management of an EEA launch and expansion, Vince has conducted deep research to build a clear product proposition, go-to-market approach, and long-term strategic vision. A Bitcoin enthusiast, he co-founded a Bitcoin mining startup that leverages excess renewable energy for power - recuperating what would have been lost effort and improving the project finance of renewables.

John McEvoy | Partner
john@valentiapartners.com

In his 25+ year career, John has delivered complex product and strategic business and technology transformations for some of the world’s largest financial institutions, working across Europe and North America. With a laser sharp focus on delivery execution, he specialises in remediating distressed transformation programmes.

Andrew Ng | Partner
andrew@valentiapartners.com

Working across business and technology advisory and transformation in Banking and Capital Markets, Andrew's experience includes designing new business units, leading complex multi-year transformation programmes, and re-shaping global operating models. As Deputy COO, he worked at C-level on an interim basis, running a technology function ($800m+ annual budget) in one of the world’s largest Universal Banks.

VALENTIA PARTNERS