DYLAN GRICE
29TH OCTOBER 2020
dylan.grice@calderwoodcapital.com

CALDERWOOD
CAPITAL RESEARCH

POPULAR DELUSIONS

"*The world is at all times the dupe of some bubble or other.*"
- Col William Rafter

IN THIS ISSUE ...

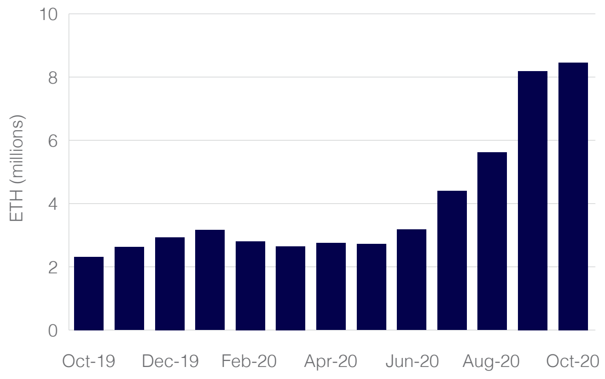
WORDS

To make good returns in the long-run you need to get to the long-run. Thus, the law of the jungle dictates that survival takes priority over reproduction.

The great unsung hero of survival is the 350m year old (and counting) cockroach which hasn't survived by being intelligent but by being robust. Several years ago, we designed a portfolio framework explicitly inspired by the lowly creature, and deliberately designed to be both dumb and resilient to extreme environments. The Cockroach Portfolio was built to survive.

Specifically, it diversified out of the biggest drivers of asset class returns to such an extent as to be largely immune from the risks embedded in any of them. In essence, it was about as risk free as you can get. So why does it make *any* kind of return at all? And why have those returns been so *astonishingly* strong over the past decade?

ETH locked in De-Fi
smart contracts



Source: DeFi Pulse

ACTIONS

Ethereum, and other decentralised platforms making use of blockchain technology, have often been mocked for providing 'a solution in search of a problem'. But last month the number of transactions on the Ethereum network hit an all time high with activity surpassing levels last seen during the 2017/18 frenzy - but this time without the ICO bubble.

We explore the renewed growth in the Ethereum economy and show that for the first time since its launch in 2015 native applications are being successfully deployed to meet native customer demand. The network without any use cases suddenly has use cases. A parallel financial system is emerging and we should all be paying attention.

REFRESHER

It's easy to get the gist of Bitcoin without understanding blockchain technology, so when we explored BTC last month we focused on its investment properties and skipped the tech. But the feedback we received from some was that an explanation would have been helpful. Moreover, to properly understand Ethereum and grasp the potential significance of what's happening on the network, it's useful to understand the basics of blockchain. We've tried to fix last month's mistake here.

A stealth flight from cash

Several years ago I'd become quite disillusioned with my life as an investment strategist in a bank. Although my job was to somehow 'know something', I'd long since reached the conclusion that I hardly knew anything. It wasn't that I was dumber or less hard-working than everyone else. It was that the future basically wasn't/isn't knowable.

It took me a while to fully absorb the implications of this realisation. But when I did, dwelling on what may or may not happen in the market stopped being as interesting to me. What fascinated me wasn't the challenge of trying to know more about the future than the rest of the market, but of figuring out how to build a portfolio given that you didn't. The challenge I grew (and remain) fascinated by was that of building a portfolio which is robust to ignorance. I found inspiration in an unusual place.

In praise of the cockroach

The lowly cockroach gets a bad press. It's unsightly, a pest, a spreader of disease … But who are we to talk? It might not be the most intelligent creature on God's earth but as a survivor, it has few peers. The first fossils date back 350 million years, which means that cockroaches have outlived dinosaurs. And as any pest-controller will tell you, they're incredibly difficult to get rid of. They can withstand ten times the radioactive dosage of humans; they can have their heads cut off and not die; you can put them in water and they won't drown because they don't need to breathe as much as we do; they can eat almost anything (including soap and wall-paper paste); and they can run at 3.4 miles per hour (5.4km/h), which is equivalent to a human running at 210mph (330km/h).

They might not have the rich trappings of intellect that we have, like literature, iPhones or edible underwear. But intellect is overrated. As a species, they're almost certain to outlive us not because they're smart, but because they're robust. This is an important insight.

Portfolio construction typically blends assets together based on their expected returns, their volatility and their correlations. The problem is that none of these variables are stable let alone predictable. Of course, that doesn't stop us trying to estimate them. The finance industry has a thriving sub-industry of prognostication and divination. But what if you just didn't bother? What if you instead absorbed the lesson of the cockroach and accepted that you didn't need to know much in order to survive? Instead of wasting time trying to understand what policy-makers might or might not do, and wasting money on advisors and research providers (except Calderwood, naturally) you could stick to a forecast you were certain will be correct: that the economy will either get better than it is today, or worse; and that inflation will either rise in the future, or fall.

Admittedly, this isn't particularly fancy. But it has the very strong merit of being true, and as such it's a good foundation upon which to build. Moreover, it's very easy to reflect in a portfolio: by allocating equally to cash, gold, government bonds and equities we can cover all of our bases (see table 1).

Table 1
How the Cockroach covers all bases

	Productive	Unproductive
Inflation	Equities	Gold
Deflation	Govt. bonds	Cash

Source: Calderwood Capital Research

Table 2 shows what the Cockroach Portfolio[1] looks like, and we'll explore some of its numbers in a moment. But for now there are a couple of interesting points to make in passing.

The first is that over the years I've been asked repeatedly by friends and family what they should do with their savings and on nearly every occasion I've recommended they build a Cockroach Portfolio using low cost ETFs. I truly think that this is the right answer for anyone who doesn't have the time, inclination or expertise to worry about markets, brokers, central banks etc. (i.e. nearly everyone alive). But almost none of them have taken the advice. They look at the Cockroach Portfolio and say 'too much gold' or 'not enough equities', which is fine, and which I understand (it's important to be comfortable with your portfolio). The thing is, when you're making judgements like those you're saying you *know* something. You *know* that you should own equities over gold, for example. And the whole point underpinning the Cockroach is that you don't.

It's true that the top-line returns look like they've been less appealing for the Cockroach than the alternatives. But bear in mind that we've seen an enormous bull market in stocks and bonds in the past four decades which has flattered their relative outperformance. The 1970s were a different story (see Table 3). As that decade drew to a close would you have worried about 'not enough equities'? If you were like most, you would probably have thought 'not enough gold.' Opinions can be dangerous. The Cockroach framework protects you by not having any.

Of course, top line returns aren't actually the whole story. It's always possible to earn higher returns by taking on more risk. It's just that this usually isn't advisable. Volatility can make you do odd things.

Table 2
Comparison of hypothetical historical returns (1973-2020)

	Cockroach	60:40	S&P500
Returns	7.9%	9.4%	10.5%
Cash Returns	4.6%	4.6%	4.6%
Volatility	6.7%	10.3%	17.5%
Max Drawdown	-17.6%	-33.8%	-55.3%
Sharpe ratio	0.5	0.46	0.34
Start date	01-01-1973	01-01-1973	01-01-1973
End date	09-30-2020	09-30-2020	09-30-2020

Source: Calderwood Capital Research

Table 3
Comparison of hypothetical historical returns (1973-1980)

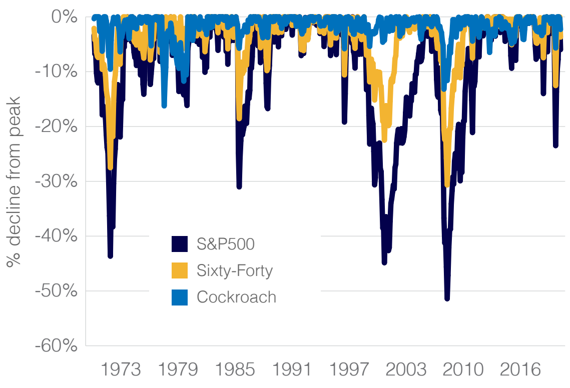
	Cockroach	60:40	S&P500
Returns	13.7%	6.6%	6.7%
Cash Returns	4.6%	4.6%	4.6%
Volatility	8.9%	9.2%	14.7%
Max Drawdown	-17.6%	-28.3%	-44.7%
Sharpe ratio	0.7	-0.09	-0.05
Start date	01-01-1973	01-01-1973	01-01-1973
End date	01-01-1980	01-01-1980	01-01-1980

Source: Calderwood Capital Research

[1] After writing about the Cockroach Portfolio, a few readers pointed out that a guy called Harry Brown had reached the same conclusion well before me, I believe in the 1980s. He had called it the 'Permanent Portfolio' (because once you've built it you don't have to rearrange it). But since I came up with the idea on my own (hand on heart) I'm going to continue calling it the Cockroach Portfolio. Mr. Brown sadly passed away some time ago, but his website is still up. It contains details of his Permanent Portfolio and assorted writings over the years. He sounds like he was a fun character who lived a good life. It would have been nice to know him. Check him out here http://harrybrowne.org/Permanent-PortfolioResults.htm

So the second thing to understand is that on this score the Cockroach does well. Not only is volatility lower and Sharpe ratio higher, but max drawdown has been *far* lower. This is something I think people don't fully appreciate. Seeing a savage drawdown when it's just a number printed on a page is easy. Living through a savage drawdown isn't. The point of maximum drawdown is usually the point of maximum madness. It typically coincides with people acting more through fear than through rational thought. It's really important to understand that such periods are stressful and that by avoiding the mental and emotional pressures induced by such panic is a very sensible pre-emptive strategy for staying rational when the time comes that those around you aren't.

Chart 1
Drawdowns compared



Source: Calderwood Capital Research

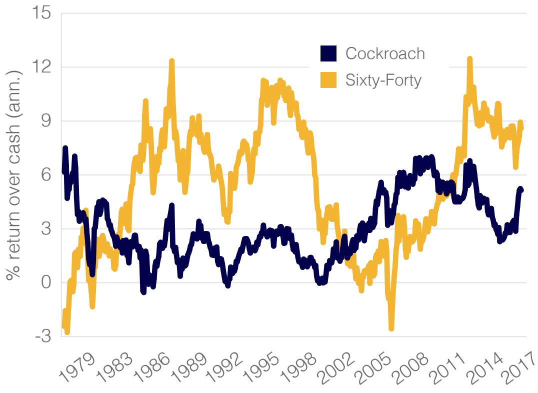
But why does it return *anything*?

As we've seen, the nature of the Cockroach framework is to cancel out the most important drivers of portfolio returns: Cockroach Portfolios survive inflationary environments as well as deflationary ones; booming economies as well as stagnating ones. This begs an interesting question: why does it earn anything at all? If hedging out all of your risk means you're not taking any risk, are you going to make any kind of return?

In theory yes. But as Chart 1 shows, when there is a crash even the Cockroach isn't going to come out completely unscathed. For the full year of 2008, for example, it returned -5% (vs -19.3% for the 60:40 and -36.9% for the S&P500). So you are taking some risk that your capital is worth less in the future than it is today. What you're paid for presumably, is for the risk of financial market exposure, and the information the Cockroach Portfolio's performance conveys is that of a generic 'financial risk premium', a base-level risk premium you can expect to harvest simply by participating in financial markets over the long run.

To give a clearer idea of how this generic financial risk premium has behaved, Chart 2 plots the rolling seven year annualised Cockroach returns over cash (3m Treasury Bills). Those for a 60-40 Portfolio are plotted for comparison. The result is quite interesting.

Chart 2
Returns over cash for two balanced portfolios



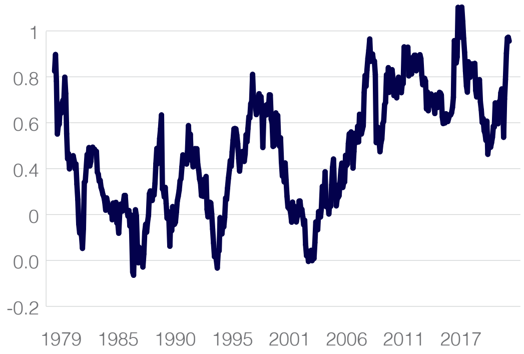
Source: Calderwood Capital Research

For starters, the excess returns to the Cockroach Portfolio show that generic financial risk premia have averaged about 3% per annum. As can be seen, it's been significantly more stable than that of the 60:40 (standard deviation of 1.61 vs 2.64).

More interesting though is that the Cockroach's excess return has risen materially over the past ten years. Specifically, in the four decades prior to the crash of 2008 its excess return was around 2% per year. But since 2010 it has been 4%. A more stark way of looking at the same phenomenon is through the Cockroach's rolling 7-year Sharpe ratio which is currently standing proudly above 1 (according to Investopedia such a reading is 'acceptable to good'[2]). So a portfolio *specifically* designed to be 'dumb' and avoid any kind of risky bet on the future – other than the generic risk of participating in financial markets - has generated the kind of risk adjusted returns most active managers would bite your hand off for (or at least those active managers with a daily mark-to-market).

Chart 3

When dumb is smart: rolling 7-yr Sharpe Ratios for the Cockroach

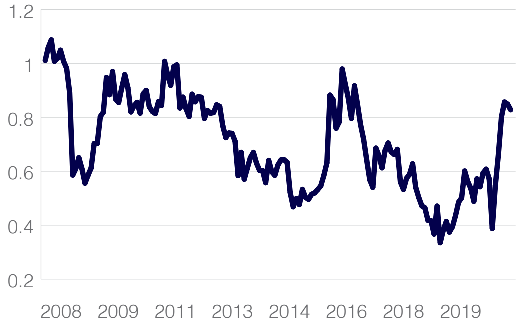


Source: Calderwood Capital Research

Note that we are focusing our attention on the US markets for reasons of data availability. But we can see something similar when we look globally. The rewards for broad and generic financial market exposure have been astonishingly high in the last ten years.

Chart 4

Rolling 7-yr Sharpe Ratios for Global Cockroach

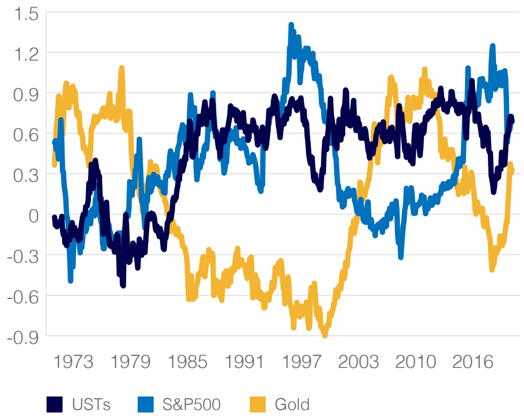


Source: Calderwood Capital Research

In broad terms, all benchmark asset classes have gone up: Chart 5 shows that the rolling 7-year Sharpe ratios for gold, bonds and equities are elevated compared to their own history, though already strong financial market returns have been turbo-charged by the strength of equity markets in recent years.

Chart 5

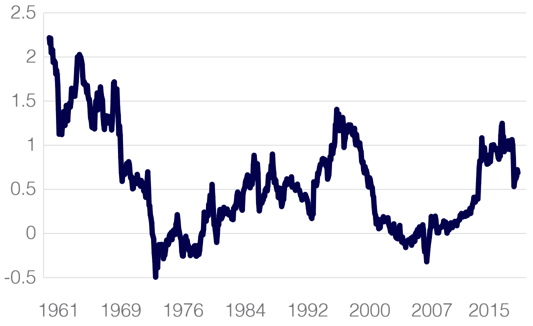
Everyone's a genius: 7yr Sharpe ratios by broad asset class



Source: Calderwood Capital Research

Chart 6

S&P500 rolling 7-yr Sharpe Ratio since the 1960s



Source: Calderwood Capital Research

This fact alone might make one deeply sceptical that this state of affairs can last, but Chart 6 should give pause for thought. It takes the rolling 7-year Sharpe ratio for the S&P500 back even further than in the other charts and shows that, by this measure, the US stock

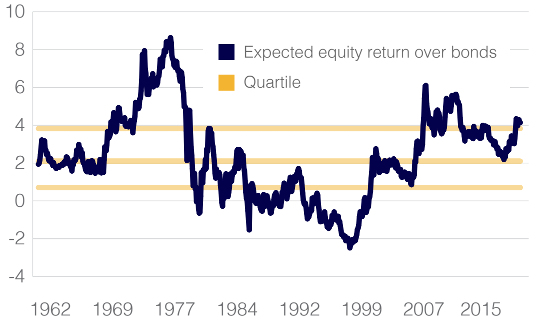
[2] https://www.investopedia.com/ask/answers/010815/what-good-sharpe-ratio.aspt

market's strength in the late 1960s and early 1970s surpassed anything that's been seen since, including the Nasdaq bubble (incidentally, this was just as Warren Buffett - then a successful hedge fund manager - was preparing to hand back his partners' capital).

Moreover, when we compare the expected return of the S&P500 (earnings_yld + inflation_breakevens) relative to those for Treasuries (yld_to_mat + roll_yield) we find them to be in the cheapest quartile relative to bonds.

Chart 7

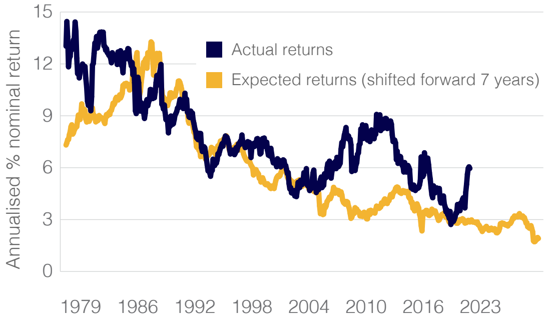
Expected equity returns over bonds in cheapest quartile



Source: Calderwood Capital Research

Chart 8

Actual vs Expected Returns for the Cockroach Portfolio

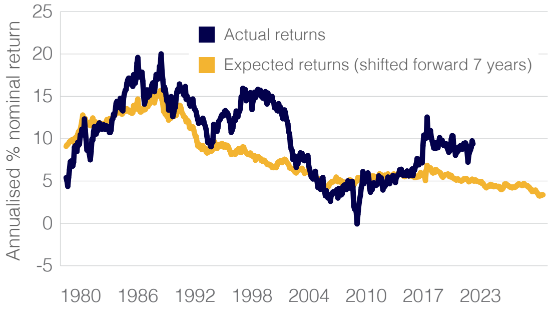


Source: Calderwood Capital Research

This makes quite a contrast to the arithmetic of expected future returns, which is sending a very strong signal that such gains are not sustainable. Charts 8 & 9 calculate portfolio level expected returns for the Cockroach Portfolio and the 60:40 and suggest that prospective returns on offer in today's market should not be expected to come anywhere close to what we've seen in recent decades.

Chart 9

Actual vs Expected returns for the Sixty-Forty Portfolio



Source: Calderwood Capital Research

Conclusions

First, the buoyant returns to indiscriminate financial market participation is strongly suggestive of a subtle but sure flight from cash. Second, equities have been the single biggest contributor to generic financial returns yet remain cheap relative to bonds. This is strongly suggestive that monetary policy is the culprit (inflation remains, for now, a Wall Street event rather than a Main Street one). Finally, the near zero expected returns across financial markets make the sustainability of today's current state of affairs suspect. Ultimately, the gravitational pull of valuation will be felt.

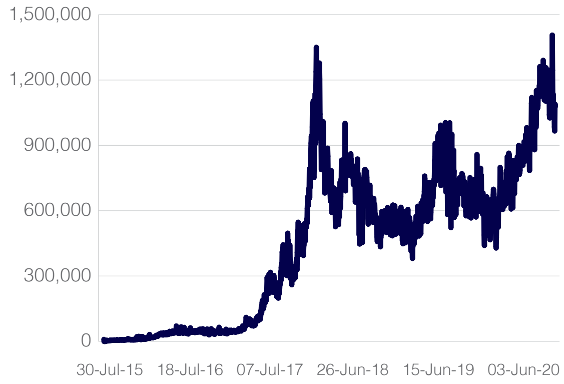
And so for the little it's worth, we continue to feel that when it comes, the culprit is likely to be more inflation than the Fed are currently bargaining for, but that for now a continued market melt-up is more likely than renewed market melt-down.

Into the Ether and a decentralised future

Last month we argued that something was stirring in the world of crypto. We focussed on Bitcoin and showed evidence of traction in places as diverse as Argentina, Venezuela and in the CME derivatives exchange. We argued that crypto is here to stay and that investors were underestimating the longevity of this newly mined asset class because they can't see its appeal, or because they don't agree with what they perceive to be its appeal.

Yet as investors, our job is to be both alert and open minded, and to us, crypto remains one of the most exciting opportunities around. So as promised, we're going to continue our exploration of the crypto complex, focusing this month on the Ethereum ecosystem.

Chart 1
Ethereum transactions



Source: etherscan.io

Chart 1 shows the volume of transactions going through the Ethereum network. If you read it from left to right you can see that transactions surged in 2017/18 during the crypto bubble reflecting the flood of new tokens which came to market during the ICO mania (the vast majority of tokens were issued on the Ethereum network). As with any bubble, the objects of the frenzy were soon revealed, with a few exceptions, to have no value. So when it collapsed, so did the flow of new ICOs and so did transaction volumes. 2017/18 transaction volumes weren't real or sustainable because the activity on Ethereum wasn't real or sustainable.

But that was then. On September 17th of this year, the volume of transactions made a new record high surpassing the previous peak of January 2018 only this time *without* an ICO bubble. Does that mean the transactions are real this time around? If so, what do they represent?

We think something interesting is happening in crypto. Specifically, a technology long-dismissed as having no relevant use-cases now has relevant use cases. This month we're going to look at some of them.

As we do, it will become clear that the Ethereum network is an economy in its own right, and as such comes with deep complexities, controversies and nuances which it's impossible to do full justice to in a short piece. So we're going to have to skip some areas which are deserving of a fuller treatment, for now at least. Nevertheless, we hope we get you to see what we're seeing, which is one of the most exciting developments in finance of our lifetimes.

Ether is programmable money

Ethereum is similar to Bitcoin in many respects: the fundamental philosophy of decentralisation, transparency and personal responsibility are as core to the Ethereum community as they are to Bitcoin's. The Ethereum blockchain is immutable and tamper-resistant, just like Bitcoin's. It records which addresses hold its native token Ether (ETH) at any point in time, just like Bitcoin's.

Transactions between addresses are validated by miners using a Proof of Work algorithm just like Bitcoin's (although the intention is to change this in time).

But there's one very important difference: smart contracts. Although the Ethereum network has addresses just like those on the Bitcoin network, where activity is determined by holders of the corresponding private keys, Ethereum has a second kind of address, except activity in the second kind of address isn't controlled by a person or not directly anyway. Activity at this second kind of address is controlled by executable code and sending ETH to such an address will trigger its code. The code at these addresses are known as smart contracts.

For example, sending ETH to one address might trigger code which asks you if you want to lend the ETH you sent (in which case your ETH earns a return) or borrow some (in which case your deposit acts as loan collateral). That code might also set a rate of interest between borrowers and lenders such that the two sides were in balance. And such an address would therefore effectively host an automated bank.

Another address might hold code which permits the sender to either underwrite a particular event (e.g. a hurricane reaching a certain speed at a particular place for a particular time) or buy insurance against that same event. Thus, that address is an automated insurance market. These examples aren't entirely made up. They are simplifications of smart contracts/ decentralised applications/'Dapps') which are being used on the network right now.

Smart contracts are what make the Ethereum network far more than 'just' a distributed ledger like Bitcoin. Smart contracts make ETH programmable money, a genuine innovation in the long history of coin, and this makes the Ethereum network very interesting indeed.

The rise of 'Decentralised-Finance'

The thing is, being 'interesting' has never been a problem for Ethereum. The challenge has been finding relevance. People less interested in idealistic visions about what the web should look like, or in replacing perfectly adequate centralised solutions with decentralised ones, or in the computer science of linking cryptography to decentralised security, just wanted something that was fun and easy to use, and which solved some kind of problem for them. And frankly, there wasn't anything.

For non-technical people, buying coins and then storing those coins safely was already a colossal headache. But so was knowing what to do with the coins you'd just bought. There wasn't much you could do with them, and nothing to use them on.

Ethereum's early years were therefore driven by speculation (what else?). And while the most visible example of this was the crypto bubble of 2017, less visible were the success stories of companies facilitating this speculation: the crypto exchanges. Don't know how to buy crypto? No problem, open an account at Kraken, Coinbase or Bitfinex and they'll buy it for you. Scared you might lose your crypto? No problem, they'll look after custody too. Not sure what to do with the coins once you've bought them? Again, no problem, trade against other crypto 'investors' and see if you can make some pocket money!

The irony was that even though these exchanges were the only success stories in the crypto space, they embodied few, if any, of the innovations around decentralisation and automation that crypto's creators had intended to unleash. The exchanges are 'conventional' businesses with little to no difference from traditional private banks: customers are KYC'd; they get an account number, a username and a password to access their account; they get access to an interface allowing them to trade for themselves; and they get access to an account manager who might help them execute large orders, advise them on which coins to buy, or on how best to deploy the coins they just bought.

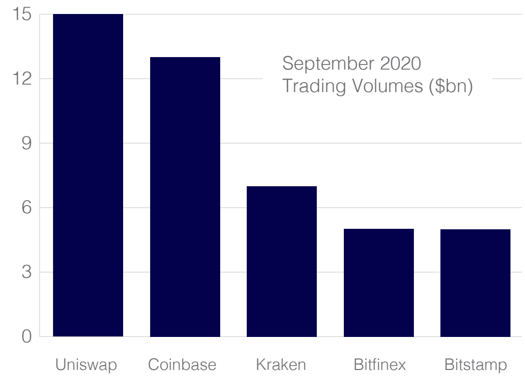
In short, there is nothing new, innovative or *remotely* decentralised about these business models (an observation, not a criticism). Yet while the ICO boom crashed and burned along with its promise to 'disrupt finance', the crypto exchanges and their undisrupted exchange-business-models went from strength to strength (crypto's rumour mill today has it that Coinbase is looking to IPO at a $10bn valuation).

This has been something of an embarrassment to many in the crypto community. Sceptics had long argued that Ethereum was built by a fringe group of computer scientists for a fringe group of computer scientists and that it would never catch on among 'normal people'. That the only crypto successes were centralised exchanges was taken as further proof that 'crypto doesn't have any fundamental use cases'.

Uniswap

As we saw, Coinbase is rumoured to be looking to IPO at a multibillion valuation. But a milestone was reached last month when Uniswap, a *decentralised* exchange ('dex'), did more volume than them (Chart 2). This is important because Uniswap is fully decentralised, fully automated and provides (as we will see) the kind of solution which is *only* possible using blockchain technology. Most importantly though, it works.

Chart 2
Uniswap volumes outpace those of Coinbase



Source: Messari

To understand Uniswap first imagine yourself a market-maker on the London dealing floor of a traditional investment bank. You hold enough inventory of the security you're making markets in to allow you to make a two-way price. The price you buy *from* the market is lower than the price you sell *to* the market and so continuously buying and selling ('crossing the spread') is where you make your profit.

The risk you're being paid for is that of sharp (and permanent) price moves. For example, a sudden price surge means everyone in the market is trying to buy. And as a market maker, that means they're buying from you, which means you're selling into a rising market. It's not a disaster because you're still selling inventory for a higher price than what you bought it for. But making markets in such an environment is costly. You'd have been better off leaving your inventory alone and enjoying the full benefits of the price move, so it's not been a good use of capital.

But declining markets are worse. With everyone selling, you find yourself accumulating inventory all the way down. If you try to adjust your excess inventory you find yourself selling into a falling market and getting less for it than you paid.

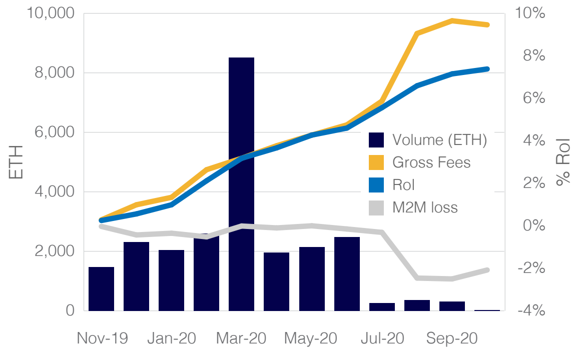
So the most profitable environment for a market maker is one in which either the price isn't moving around or it is, but those prices are highly mean-reverting. The point being that the return on market-making inventory has a particular pay-off profile which isn't structurally different from a vanilla buy-and-hold profile.

Now, what Uniswap does is completely automate this entire process. Thus, it makes two-way prices which allow traders to buy and sell tokens, in the same way they might buy or sell tokens anywhere else: input the ticker, the number of tokens to trade and hit buy or sell. But what Uniswap also does, and does uniquely, is that it allows anyone to participate in the *funding of inventory*. Indeed, if there is no-one to fund the inventory, there is no liquidity in the token.

So instead of leaving coins idly in your wallet you can commit them to a Uniswap liquidity pool which will be used to provide inventory for a simple market-making algorithm Uniswap traders can use to buy and sell. In return for committing your coins you receive a token representing your share of the liquidity pool. There is no lock on your contribution, which you can withdraw at any time. Each trade costs 30bps of the transaction value which accrues to the pool.

So the value of the pool rises as there are more transactions, and falls if there are sudden moves in the underlying token value. As a liquidity provider contributing inventory to facilitate Uniswap's automated market making facility, you're now being paid to take similar risks to those on the London bank dealing floor.

Chart 3
Uniswap ROI for ETH/WBTC pair



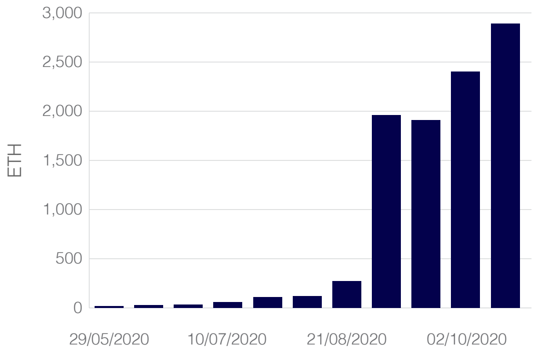
Source: www.zumzoom.github.io

A sceptic might point out that for all its elegance, Uniswap still isn't a real use case. It's still mainly punters trading against each other. But this misses the point. There is a legitimate demand for token trading and until now that demand has been supplied by traditional business models, the most prominent of which is Coinbase. But if Uniswap surpassed Coinbase's September market share, Uniswap presumably has also created several billion dollars of value. Yet the decentralised nature of its model means that that value is being realised by its users, almost as though it were a mutual.

Note the following:

- The process is fully automated[1]
- It is fully decentralised (no banks, brokers or prop-shops)
- It is completely democratic (the returns to risk-bearing are as accessible to someone contributing $100 as they are to someone contributing $1m, and value accrues directly to its users)
- It is *completely* native to the blockchain (how would you do this in the traditional 'fiat' space?)

Chart 4
Trading inventory locked in Uniswap smart contracts



Source: Uniswap

As it happens, the criticism is misplaced in another respect. Some of the most successful and widely adopted protocols to emerge this year are those which natively generate a more conventionally stable yield. Remember earning 4-5% per year on your USD current account deposits? Well you still can in the Ethereum network.

DAI

Ether and Bitcoin are infamously volatile, but the Ethereum network, being the creative capitalist commons that it is, already comes with several solutions and there are plenty of coins with the sole purpose of reliably pegging to the dollar (so called 'stablecoins'). Probably the best known of these is Tether which operates kind of like an ETF with each newly minted Tether coin backed by 1 USD.

On one level, Tether isn't very interesting. It is a classically centralised solution with a single point of failure and doesn't embody or encapsulate any of the decentralised potential which blockchain technology enables. On another level though, Tether is very interesting, because a) it is under investigation by the New York State Attorney for fraud, and b) it currently represents around half of all crypto trading volumes. Tether is interesting for the wrong reasons, and as a topic it

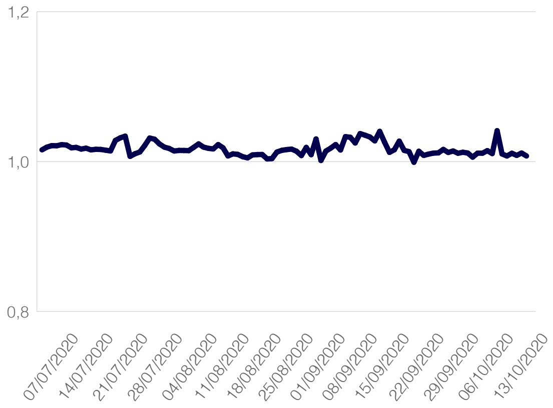
[1] We won't go into the details of the market making algorithm here (a 'constant product' algorithm) but it is impressively simple: no order book and no matching algo. A study by Standford's Guillermo Angeris concluded "Though simple, constant product markets and their generalizations have very nice theoretical properties (such as fairly strict no-arbitrage bounds on the reference price) which appear to hold in practice.'" See https://arxiv.org/abs/1911.03380

deserves its own piece. So it's likely we'll spend some time in a future edition looking more closely at it, but for now we're going to focus on the good things happening on the network.[2]

DAI coin gives a far better example of how blockchain can enable a 'clean' stable coin. It's operated entirely by smart contracts and uses well-designed incentive mechanisms to ensure that the value of one DAI remains closely aligned to 1USD. We don't have time to go into how that mechanism works here[3], but chart 4 shows that it generally works quite well (although as can be seen, DAI has been trading at a premium in recent months which in itself is an interesting side story, and related (very) tangentially to the Tether story but again, we will leave a thorough explanation of this for another time).

Chart 5

DAI USD exchange rate



Source: Coinmarketcap.com

The point is that being on the Ethereum network doesn't mean you're restricted to using ETH. You can move into any supported currency you like including more stable ones. And the reason you might want to do that is because, like we said, you can still get a return on deposited funds using lending protocols like those listed in Table 1.

Compound is the largest such protocol. It is a smart contract which matches borrowers with lenders by setting a continuously adjusting interest rate to balance them. Aave achieves the same outcome but with a different back-end: as a depositor you place your DAI (or whatever) into a pool in return for a token which gives you your share of that pool. Borrowers borrow from the pool sending interest into it each day. Because it works via this pool there's no duration to the deposit or the loan. If people withdraw from the pool, the supply of loanable funds shrinks and interest rates increase. If lenders pay back to the pool, the opposite happens, and rates decline. Default risk is basically zero because borrowers have to over-collateralize their loan. And it being crypto, if the collateral price moves against the borrower to reach the collateral limit, it will automatically be liquidated to repay the loan. The Aave smart contract manages the pool.

Table 1

USD lending rates

	Lend	Borrow	$m outstanding
Compound	2.8%	3.9%	966.82
Maker	0.0%	3.3%	938.78
Aave	4.3%	6.5%	16.35
dYdX	4.0%	6.6%	3.89

Source: defipulse.com

Is the ability to earn 4-5% on your demand deposits *massively* exciting? No. But it's not to be sniffed at either. We don't need to remind subscribers that most government bonds yield a negative return. IG corporate bonds yield less than 2%. A reasonable expected return for equities here is 5%. Isn't it worth doing some homework into crypto to consider a 4-5% return per year?

[2] Tether's holding company is currently the subject of a class action complaint blaming it for inflating the ICO bubble and misrepresenting its financial position to investors. Full documents here https://www.courtlistener.com/recap/gov.uscourts.nysd.524076/gov.uscourts.nysd.524076.1.0.pdf
It is also under investigation by New York State Attorney General Letitia James for fraud https://ag.ny.gov/press-release/2019/attorney-general-james-announces-court-order-against-crypto-currency-company

[3] If you're serious about getting involved in this space you really should understand how the Maker protocol works. Go here to learn all about it https://makerdao.com/en/whitepaper/

Hack insurance

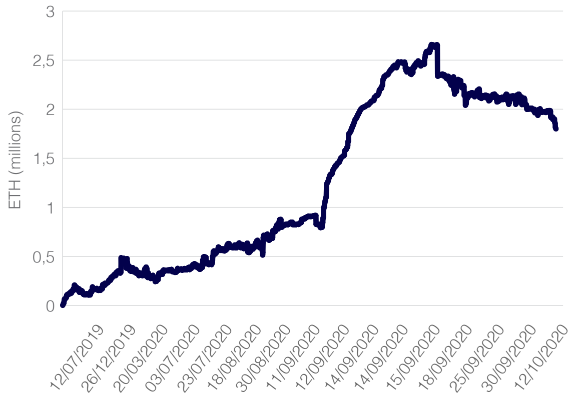
The important difference between contributing some of your coins to a Uniswap liquidity pool or an Aave smart contract versus a boring old bank deposit is that if the bank gets hacked it's their problem not yours. And if the bank goes bust your deposits are insured up to a limit depending on which country you're in.

You don't get that comfort in crypto. If the smart contract is hacked you're on the hook for losses. Not that there have actually been many smart contract hacks during Ethereum's existence so far (the most high-profile hacks have been of centralised exchanges). And it is now standard practice to have multiple pre-deployment external code audits completed before launch. Nevertheless, the amount of collateral locked in decentralised finance smart contracts has exploded this year and as we write, we can be sure that someone somewhere is poking around GitHub repositories looking for smart contract vulnerabilities they can exploit. With around $10bn locked in smart contracts the question is 'when' not 'if' a hacking attempt is made on one of them.

But trade has always been risky. And so long as that risk has been a barrier to doing business, there have been insurance markets. In Babylonian times, the Code of Hammurabi (c.1750BC) specified how traders, for an additional fee, could request their loans be cancelled should their shipment be lost at sea. Today, Nexus Mutual, an entirely on-chain insurance mutual provides cover against smart contract-hacks, not by underwriting any of the risks itself, but by allowing token holders (i.e. mutual members) to stake their tokens as collateral against the event happening over a designated period of time, earning a premium when the event doesn't happen.

Again, we don't have the space this month to do the Nexus model anything like the service it deserves but what is emerging is similar to what we've already seen: highly automated (the smart contract manages the mutual), highly decentralised (community members contribute their capital and are rewarded for the risks borne), carefully designed incentive mechanisms, and most importantly, a native solution to a native problem. Chart 6 shows that Nexus is currently insuring around ETH2m, or around 25% of the ETH collateral held in smart contracts.

Chart 6
Nexus Mutual insurance cover



Source: Nexus Mutual

Putting it all together

So what are the investable actions here? We've briefly touched on some interesting smart contracts, and token-based business models, but what do we actually *do* differently?

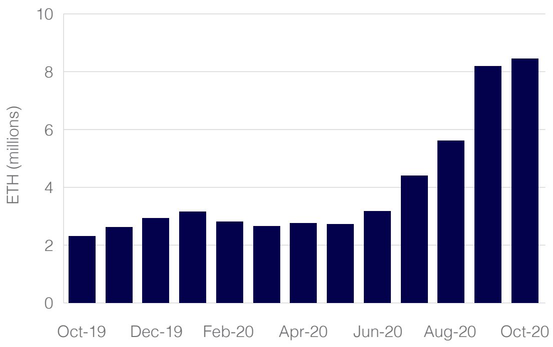
The first thing to say is probably the most obvious: we own ETH because we think the Ethereum network is here it stay. Those developers building applications on the network are intelligent, thoughtful and motivated. They're building creative solutions to user problems which are increasingly native and as such, we are seeing the first baby steps not just of a parallel financial system but of a new internet. 10% of ETH is already locked in smart contracts, which means that 10% of ETH has essentially been removed from supply. As development accelerates, more capital will be locked in more smart contracts, meaning the circulating supply will diminish

[4] The highest profile hack was in 2016, when the 'Decentralised Autonomous Organization' (DAO) was hacked for what was then a staggering 14% of all ETH tokens in issue. As it happened, the DAO was a terrible idea (a venture fund which would make investment allocations based on the voting preferences of its 11,000 token holders) so maybe the hack did everyone a favour. And, controversially, the hacker was hard-forked out of his or her gains. A more recent hack involved a smart contract built by Ethereum co-designer Gavin Wood's Parity, although this seemed to be more a coding error from someone at Parity who accidentally permanently locked some of the firm's ETH.

proportionately. We own it for this reason (and when I say 'we', I mean my wife and I, not the fund Calderwood is in the process of launching).

Chart 7

ETH locked in De-Fi smart contracts



Source: DeFi Pulse

There may be better ways to gain exposure to smart contract growth though. As things stand, ETH supply is also growing at around 10% per year and that's likely to continue until the blockchain's validation mechanism moves from its current Proof of Work to the long awaited Caspar Protocol (a Proof of Stake protocol). This move will be very bullish for the coin and for the ecosystem in our view. But it's been in the pipeline for several years now, and delays have become the norm. In the meantime, that 10% inflation is quite a headwind.

Individual tokens might offer more upside too. We briefly touched on Nexus Mutual (NXM), the insurer of smart contracts. Presumably, as the universe and traction of smart contracts grows, the business opportunity for NXM does too. Indeed, NXM see smart contract underwriting as its first gambit. When the infrastructure is in place, it expects to move into the underwriting of more traditional and likely parametrically definable insurable events. We expect to explore some token-specific ideas along these lines in coming months, but in the meantime, NXM and ideas like it are highly idiosyncratic and require a significant amount of work to understand properly.

The lending protocols seem interesting too. On the surface, earning 4-5% for dollar deposits seems like a no brainer. What's to stop you from taking any cash deposits you have from the bank, sending them to Coinbase, Kraken, Bitcoin Suisse (or wherever you have your crypto account), telling them to buy you some DAI, and stashing them in Compound, Aave, or a Uniswap pool? The answer, for us at least, is that those smart contracts aren't yet battle-tested. Caution makes sense before deploying meaningful amounts of capital here.

What doesn't make sense is doing nothing. The best learning is doing. So by all means dedicate some time to reading about the Ethereum network, or watching videos about it. But perhaps the best investment you can make is to spend some time *using* it. If you haven't already opened an account at a crypto broker, do it now. Set yourself up with a MetaMask wallet and put your crypto in that. Then start exploring the decentralised Web. You might be surprised at how quickly you start to prefer it to the traditional web.

Sharing is caring

Dear Subscribers, as a reminder, we write about ideas in this section which we're either invested in already, or actively considering investing in. Typically, we invest through allocations to managers we know but occasionally we will invest directly in the idea and this section is as much about figuring out our own thinking as it is about sharing some of the more interesting ideas in our deal flow. If you think we're missing something or have made a mistake in any of the theses you read here, or if you are seeing better opportunities elsewhere, please don't be shy about reaching out directly.

Email to dylan.grice@calderwoodcapital.com. We are accredited investors, and all correspondence will be treated in strict confidence.

Blockchain for dummies

Last month we didn't spend any time explaining how Bitcoin works, and instead gave a few YouTube links to people who felt the need to educate themselves. But we received a few complaints from subscribers who thought we'd assumed too much knowledge. So here we try to fix that mistake by giving a quick overview of what happens on a blockchain, and why blockchains have the properties they do.

Solving the 'double-spend' problem

The simple place to start is to think about what happens when you email someone an electronic file. The act of emailing the file doesn't mean you no longer have that file. Indeed, you can send it on to as many people as you like and you'll still have the file afterwards. This is a good thing for most files. It means that doing something like sending birthday photos around to your family is easier and cheaper than it would be if you had to go print each photo and then physically send them. But it's not so good for digital assets, which have to be non-reproducible in order to ensure that any dollars can't be copied and spent again (the 'double-spend' problem).

You might not be fully aware of the problem as it relates to currency because you're familiar with paying a merchant with your Visa card, or sending money to a friend using PayPal. Don't we already have digital payments? Well kind of. Those corporations, and many like them, do allow you to send money around, and sometimes quite fast. But they never actually solved the double-spend problem.

Instead, they use a work-around solution by coordinating with the banks to make sure that your new bank balance and the merchants' new bank balance accurately reflect any transaction. So if you send me $100, your bank confirms that you're legitimate and that you have the necessary funds while my bank confirms that I'm legitimate and have an account capable of accepting those funds. Once our banks agree, your bank lowers the ledger it holds on your behalf (i.e. your bank account) by $100, while my bank increases the ledger it holds on my behalf by $100. This is how digital payments work in the traditional payments system.

Although it functions pretty well, it can be slow and sometimes quite cumbersome (as anyone trying to send money internationally will be able to attest). And of course there's always that nagging concern about what the bank is *actually* doing with your money and whether it will be there tomorrow (Bitcoin was released in the teeth of the 2008 banking crisis).

The Bitcoin protocol solves the double-spend problem in a very elegant way. A single ledger of each account's token balance (i.e. *the* ledger, rather than a collection of ledgers held at various intermediaries) is maintained on a network of computers. That ledger is freely available to anyone who wants to look at it, download it or be a part of the network (although it's not known who owns those accounts unless the account owner makes that information public, so it is also anonymous).

Now, if you want to send me one bitcoin (BTC), you access your account (i.e. your public address) with your private key, enter my account details (i.e. my public address) and hit send. That action broadcasts your intention to the network which now gets to work making it happen.

Each computer sees the same proposed transaction and each computer has the same version of the existing ledger, each computer can calculate what they think the new ledger should look like. Therefore, if the transaction is legitimate (i.e. you had the 1 BTC to send in the first place, I had a valid account to receive the funds) the computers in the network should arrive at the same post-transaction ledger. Therefore, assuming you had the 1 BTC to send, and I have a valid address, the network will be able to confirm the transaction as valid. The new ledger will therefore show that I now own 1 BTC more than I did before the transaction, and you own 1 BTC less.

No banks were involved. Indeed, we don't even have bank accounts. Just addresses on the network. The only 'middle men' were the computers on the network which confirmed the transaction to be valid (and would have rejected it if it wasn't).

The computers in the network perform such a benign service because they are incentivised to do so by the protocol. Specifically, each validating computer in the network is incentivised to be the *first* to confirm that the transaction checks out. Solving the puzzle requires the use of brute-force computational power, and so this validation method is called 'Proof of Work'. And although the puzzle takes some time to solve, it only takes a moment to validate (in the same way that figuring out which two numbers multiply together to reach 7,636,969 would take even a number theorist several minutes, but that verifying those two numbers are 1,033 and 7,393 takes a second). Thus, the first computer to find a solution to the puzzle which the rest of the network accepts earns a fee. The transaction is then recorded in the updated ledger, that ledger is adopted across the network as now being *the* ledger and the new ledger will now form the basis of future transactions.

Could you cheat? Could you plug your own machine into the network and sneak in your own little adjusted ledger, one which gave you an extra 1 BTC, and which you hope no one notices during the next round of transaction validations?

The clever thing about the puzzle all the network computers have to solve is that it embeds both the transaction data and the current state of the ledger as variables. This means that if you put in the wrong variable for the transaction (e.g. 2 BTC instead of your 1 BTC account balance), or for the state of the ledger (e.g. that you own one bitcoin more than you do), you can't get the right answer. So you'll never find a solution the rest of the network can validate and your version of the ledger will never be accepted as *the* ledger.

Moreover, if you tried to run with your version anyway you'd never solve future puzzles, because by constantly working with the wrong input you'd never get the correct output. So not only would you no longer be in the running for future mining fees, but the ledger which shows you have an extra bitcoin wouldn't be worth anything. So you wouldn't have the extra bitcoin either.

In practice, transactions aren't validated one at a time. They are validated in blocks of transactions. Each version of the ledger forms the basis for calculating the next block. Hence: blockchain.

Blockchain's personality

It's important to understand this before trying to understand Ethereum. Although Ethereum is a more complex animal it is still a public blockchain, inspired by Bitcoin, so the core ethos and the fundamental characteristics are the same. Understanding these characteristics might help you better understand the unique culture you find in the crypto community.

The first and most important is the decentralised nature of the solution. There is no central authority guiding the system's activities or enforcing good behaviour among its participants, just well-defined incentives applied to all members equally. Since centrally controlled systems are more vulnerable to attack or corruption as they have a single point of failure, decentralised systems are more robust and less corruptible. In crypto, therefore, the conviction that decentralised solutions are always and everywhere superior to centralised ones is core and generally non-negotiable.

A second, and related aspect, is that decentralised peer-to-peer solutions can be elegant and are preferable, removing unnecessary intermediaries (banks in the case of financial transactions, but wider examples emerge when you explore Ethereum). A third is that the blockchain is immutable: every past state of the ledger has been validated as being correct in the same way that the current state of the ledger is correct. No one can claim that you don't own what you own, or that they own what they don't. The blockchain is the truth, clean and incorruptible.

The final one is that each individual is responsible for their own actions. The only way to access an address is by using the unique private key which corresponds to that address. Although some solutions are emerging (decentralised solutions, naturally) there's no system administrator who can 'reset' your password. If you lose the private key, you lose access to that address. This spirit of self-reliance and user-sovereignty is a defining characteristic in crypto.

DISCLAIMER & DISCLOSURE STATEMENT

THIS MATERIAL IS: (I) FOR YOUR PRIVATE INFORMATION, AND WE ARE NOT SOLICITING ANY ACTION BASED UPON IT; (II) NOT TO BE CONSTRUED AS AN OFFER OR A SOLICITATION OF AN OFFER TO BUY OR SELL ANY SECURITY IN ANY JURISDICTION WHERE SUCH OFFER OR SOLICITATION WOULD BE ILLEGAL; AND (III) BASED UPON INFORMATION THAT WE CONSIDER RELIABLE.

CALDERWOOD CAPITAL RESEARCH DOES NOT WARRANT OR REPRESENT THAT THE PUBLICATION IS ACCURATE, COMPLETE, RELIABLE, FIT FOR ANY PARTICULAR PURPOSE OR MERCHANTABLE AND DOES NOT ACCEPT LIABILITY FOR ANY ACT (OR DECISION NOT TO ACT) RESULTING FROM THE USE OF THIS PUBLICATION AND RELATED DATA. TO THE MAXIMUM EXTENT PERMISSIBLE ALL WARRANTIES AND OTHER ASSURANCES BY CALDERWOOD CAPITAL RESEARCH ARE HEREBY EXCLUDED AND CALDERWOOD CAPITAL RESEARCH SHALL HAVE NO LIABILITY FOR THE USE, MISUSE, OR DISTRIBUTION OF THIS INFORMATION.

The analysis and information presented in this report (Report) by Calderwood Capital Research, is offered for subscriber interest only. The content is intended for sophisticated investors only. By accessing this Report you confirm that you meet these criteria.

This Report is not to be used or considered as a recommendation to buy, hold or sell any securities or other financial instruments and does not constitute an investment recommendation or investment advice. The information contained in this Report has been compiled by Calderwood Capital Research from various public and industry sources that we believe to be reliable; no representation or warranty, expressed or implied is made by Calderwood Capital Research, its affiliates or any other person as to the accuracy or completeness of the information. Calderwood Capital Research is not responsible for any errors in or omissions to such information, or for any consequences that may result from the use of such information. Such information is provided with the expectation that it will be read as part of a wider investment analysis and this Report should not be relied upon on a stand-alone basis. Past performance should not be taken as an indication or guarantee of future performance; we make no representation or warranty regarding future performance. The opinions expressed in this Report reflect the judgment of Calderwood Capital Research as of the date hereof and are subject to change without notice.

This Report is not, and should not be construed as, an offer or the solicitation of an offer to buy or sell any securities. The offer and sale of securities are regulated generally in various jurisdictions, particularly the manner in which securities may be offered and sold to residents of a particular country or jurisdiction. Securities referenced in this Report may not be eligible for sale in some jurisdictions. To the fullest extent provided by law, neither Calderwood Capital Research nor any of its affiliates, nor any other person accepts any liability whatsoever for any direct or consequential loss, including without limitation, or lost profits arising from any use of this Report or the information contained herein.

Calderwood Capital Research Ltd is an appointed representative of Messels Ltd which is authorised and regulated by the Financial Conduct Authority. This report is intended for professional clients only, as defined by the Financial Conduct Authority.

This Report, including the text and graphics, is subject to copyright protection under English law and, through international treaties, other countries. No part of the contents or materials available in this Report may be reproduced, licensed, sold, hired, published, transmitted, modified, adapted, publicly displayed, broadcast or otherwise made available in any way without Calderwood Capital Research's prior written permission. All rights reserved. This document is produced using open sources believed to be reliable. However, their accuracy and completeness cannot be guaranteed. The statements and opinions herein were formed after due and careful consideration for use as information for the purposes of investment. The opinions contained herein are subject to change without notice. The use of any information contained in this document shall be at the sole discretion and risk of the user. Investors should consider this report as only a single factor in making their investment decision and, as such, the report should not be viewed as identifying or suggesting all risks, direct or indirect, that may be associated with any investment decision.

No liability whatsoever is accepted for any loss arising whether directly or indirectly as a result of the recipient acting on such information or opinion or estimates. Calderwood Capital Research employees may have or take positions in the markets, securities or other investments mentioned in this document. The stated price of any securities mentioned herein is not a representation that any transaction can be effected at this price. Investing entails risks. The investments referred to are not suitable for all investors and should not be relied upon in substitution for the exercise of independent judgment. This material is not directed at you if Calderwood Capital Research is prohibited or restricted by any legislation or regulation in any jurisdiction from making it available to you. Calderwood Capital Research and its analysts are remunerated for providing independent investment research to financial institutions, corporations, and governments.

DISCLOSURE: This Report is not to be copied, forwarded or otherwise disseminated to non-subscribers in electronic or physical form without prior consent.