The Economist

Elon Musk's wood-chipper

How Trump could still blow up global trade

Taking MAGA to Gaza

The economics of fake diamonds

FEBRUARY 8TH–14TH 2025

SCAM INC

How the world's most dangerous illegal industry really works

Business

Photograph: Getty Images

Donald Trump announced and then postponed punitive tariffs of 25% on goods from Canada and Mexico. The American president is using the threat of tariffs to press both countries to stop the flow of migrants and fentanyl across the border. He granted a 30-day reprieve following urgent talks with Claudia Sheinbaum, Mexico's president, and Justin Trudeau, Canada's prime minister. Both leaders promised to boost their border security. Both had earlier vowed to retaliate with tariffs of their own on American products. The European Union said it would also retaliate after Mr Trump said he would "definitely" impose tariffs on EU imports over America's trade deficit with the region. Global markets shuddered.

The phoney war

Mr Trump did impose extra tariffs of 10% on Chinese imports. China responded with limited duties on a range of American goods, tighter export controls on critical minerals and an antitrust investigation into Google, which has little presence in China. Its muted response raised hopes that the two sides will negotiate.

The tremors from the political earthquake in Washington spread to the Consumer Financial Protection Bureau, a watchdog that the Republicans have wanted to abolish ever since its creation after the global financial crisis of 2007-09. Donald Trump dismissed Rohit Chopra as head of the bureau and Scott Bessent, the treasury secretary, took over as acting director. Mr Bessent immediately put the CFPB's investigations and proceedings on hold.

The chief executive of Hewlett Packard Enterprise, Antonio Neri, said his company would fight the Justice Department's attempt to block its $14bn acquisition of Juniper Networks. The department's lawsuit claims the takeover would reduce competition in the market for networking equipment, but Mr Neri said its reasoning is flawed. The deal has already been approved in Britain and the EU.

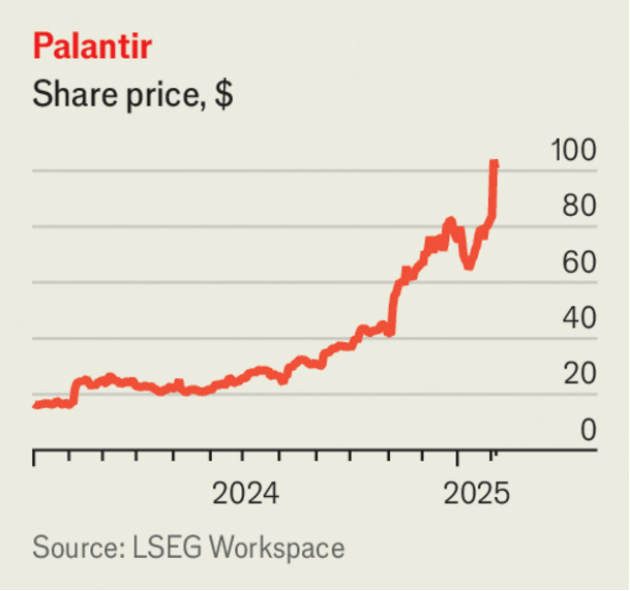

Chart: The Economist

The share price of Palantir surged to a new high, after the data-analytics company produced a bumper set of earnings and described demand for its artificial-intelligence software as "untamed". The company focuses primarily on the defence industry and has benefited from the election of Mr Trump. Alex Karp, the CEO, described the new government's cost-cutting drive as a "revolution", which would benefit Palantir because of its data-crunching expertise.

By contrast, Alphabet's stock sank after its quarterly earnings disappointed investors. Revenue from its cloud business grew by 30%, year on year, but this was less than the 35% in the previous quarter. Alphabet suggested it didn't have the capacity to meet demand. It also anticipated investing $75bn on data centres this year, up from $53bn last year.

What market rout in AI?

OpenAI and SoftBank announced a venture that will develop AI across the Japanese conglomerate's subsidiaries. SoftBank is investing $3bn a year in the project, named Cristal Intelligence. Its aim is to create AI agents for "knowledge work" that will automate mundane tasks, such as generating financial reports and managing customer inquiries. It will also be marketed to other companies in Japan. Masayoshi Son, SoftBank's boss, said he now believes that the ability of AI to match or surpass humans across a range of cognitive tasks will happen much sooner than he had predicted.

The Bank of England reduced its benchmark interest rate from 4.75% to 4.5%. Two members of the monetary committee voted for an even larger cut of half a percentage point. The bank said that inflation in Britain remains "somewhat elevated", and economic growth "has been weaker than expected".

The release of "Moana 2" and "Mufasa: The Lion King" helped Disney's earnings come roaring back to life in the last three months of 2024. Operating income at the company's entertainment division, which includes films, grew by 95% in the quarter, year on year. Revenue from streaming was up by 9%. "Inside Out 2", "Deadpool & Wolverine" and "Moana 2" were the top three box-office hits worldwide in 2024.

Quarterly revenue and profit at UBS came in above market expectations, which the Swiss bank said was a result of strong demand from institutional and private clients following the election of Mr Trump. It warned, however, that its plans for a $3bn share buy-back could be derailed by possible higher capital requirements in Switzerland.

UPS announced that it was reducing the amount of shipments it handles from Amazon by 50% so that it can focus on more profitable business. The US Postal Service recently adjusted its fees, shaking up the economics of parcel deliveries. We are "taking control of our destiny", said Carol Tomé, the chief executive, before UPS's share price sank by almost 15%.

Spotify reported its first annual profit since launching in 2008. The music and podcast streaming platform now has 675m monthly active users.

Finance & economics
It's not over: Donald Trump could still blow up global trade

Ideology, complacent markets and a need for revenue may still lead to big tariffs

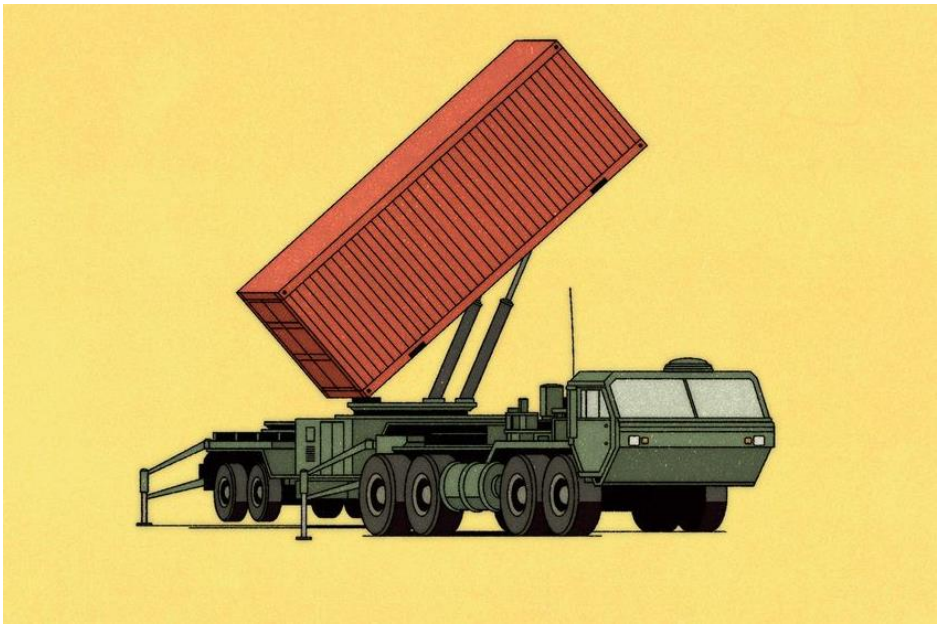

Illustration: Álvaro Bernis

IF DEALMAKING MEANS threatening catastrophe in order to win small gains, then Donald Trump is the master of the art. Having threatened Canada and Mexico with 25% tariffs which would have imperilled the carmaking that criss-crosses North America's borders, he granted them both a 30-day reprieve on February 3rd. In return, he got a modest boost to their help securing America's frontiers, including from 10,000 extra Mexican troops, plus the reiteration of some old promises.

Was the "dumbest trade war in history" also the shortest? Investors seem to think so. For months they saw Mr Trump's threats as negotiating ploys. Then, as tariffs loomed, the S&P 500 index of American stocks fell by 3%. But since the first deal with Mexico they have recovered their poise, and more than half their losses.

Unfortunately, that looks like complacency. It would be a mistake to conclude Mr Trump's trade aggression is a tactical distraction. More probably, it is only just getting started.
For one thing, a blanket 10% tariff really did go into effect against China—adding more than half as much again to existing average levies on the country. China has set out its retaliation, which will come into force on February 10th. And Mr Trump has vowed to strike more blows, including, perhaps, to fulfil his threats against the European Union and Taiwan.

For another thing, the president genuinely believes that tariffs would be good for the American economy. It is true that in his first term Mr Trump repeatedly backed out of tariff threats; America's effective average tariff rate rose by just 1.5 percentage points. Ever the showman, he delights his base by throwing America's weight around and boasting of his victories.

However, he repeatedly sets out his vision for the re-industrialisation of America by force. He wants manufacturers to choose between tariffs and moving production to America—which he promises will be a low-tax, deregulated business paradise. He also castigates countries with which America runs trade deficits, which he calls "subsidies", as if buying from a foreigner involved a gift rather than a beneficial transaction. And he has extolled the federal budget of the late 19th century, under presidents including William McKinley, when America's federal government raised much of its revenue from tariffs because there was not yet a federal income tax.

That leads to the biggest reason to fear tariffs, which is that the federal government needs the money. Its deficit in 2024 was 6.9% of GDP. Official forecasts show this remaining above 5%, despite assuming that many of Mr Trump's tax cuts from his first term will expire as scheduled at the end of 2025.

In reality Republicans want to renew those tax cuts and then some. Mr Trump is odd in his belief that tariffs are desirable on their face. But plenty of Republicans may prefer them to defying him and putting up income taxes. A 10% universal tariff would raise about 1% of GDP in annual revenue—not much less than the cost of renewing Mr Trump's earlier bill. Today's rules prevent a simple majority in Congress from passing budgets that raise deficits more than ten years into the future. So if universal tariffs were in the law, it might enable permanent tax cuts. As a result, although it is impossible to imagine a wholesale return to the 19th-century tax system—not least because America's government is a far bigger share of the economy—a step in that direction is all too plausible.

The blow to the global economy would be profound. Mr Trump is right that America holds the cards in a trade war. It is an enormous, diverse free-trade zone with plentiful natural resources. The big costs of a step towards autarky would be borne by places that depend on America for trade, none more so

than its immediate neighbours. However, the Smoot-Hawley levies that helped wreck global trade in the 1930s raised America's tariff rate by only six percentage points, and from a much higher starting-point. Their effects were exacerbated by deflation and the retaliation against America that followed. Thankfully, today's world economy is much healthier, but retaliation is still certain. And if a trade war can rage when there is no global slump, what happens when a recession hits?

Hold your fire

Mr Trump is sensitive to Wall Street's opinion, viewing the stockmarket as a kind of presidential scorecard. If it concludes that he is always bluffing when he threatens self-harming policies, it will fail to move—making him think it is safe to follow through. Expect, therefore, that the president will take the global trading system to the cliff edge repeatedly, each time with a growing risk that he pushes it over.

How to invest like a MAGA bigwig

Cannabis, crypto or half of North Dakota?

Illustration: Satoshi Kambayashi

When the 24 cabinet secretaries and top-level officials in Donald Trump's new government assemble, they will form one of the wealthiest administrations in history. Whether they are the very wealthiest is impossible to say, since official disclosures top out at "over $50m"—a pittance for some of the assembled. But such disclosures are helpful in another way: they shine a light on the widely varying investment strategies of MAGA luminaries, and thus their widely varying outlooks on the world.

For many, the lion's share of their wealth is held in private firms. This is true of two of the richest: Howard Lutnick (Mr Trump's nominee to be commerce secretary) and Linda McMahon (the education nominee), whose wealth is counted in the billions. Mr Lutnick is chairman of Cantor Fitzgerald, a brokerage and investment bank. Ms McMahon, whose finances are yet to be disclosed, owes most of her riches to World Wrestling Entertainment, a sports-media business. At the other end of the spectrum, Lori Chavez-DeRemer (labour) owns a stake worth between $1m and $5m in SJJD Consulting, a recreational-cannabis producer with a licence to operate in Oregon, her home state.

Property investments are another recurring theme. Most cabinet members and would-be members are landlords; none is more enthusiastic than Doug Burgum, the secretary of the interior. Twenty-four years ago he sold Great Plains Software, a technology firm, to Microsoft for $1.1bn of the computing giant's stock. He has since bought up swathes of land across his home state of North Dakota and neighbouring Montana, which will have appreciated nicely: house prices are on the rise in both states. He would have been better advised to keep hold of the Microsoft stock, however, which has risen in value by more than 1,200% since he sold his company.

That is where the similarities end. The most obvious differences concern overall levels of wealth. Scott Bessent, a hedge-fund titan whom Mr Trump has selected as treasury secretary, owns art and antiques worth $1m-5m, or at least five times the value of all assets reported by Marco Rubio, America's secretary of state. Mr Bessent has holdings in stock and bond exchange-traded funds (ETFs), and hundreds of millions of dollars in bets on international currency markets. The latter is a meat-and-potatoes choice for a hedge-fund magnate, even if it would be a little adventurous for an average retail investor.

The portfolios of Jamieson Greer, Mr Trump's nominee to be US trade representative, and John Ratcliffe, the new director of the CIA, are largely held in pedestrian stock and bond funds, bank accounts and annuities, as well as a few individual stocks. By contrast, some MAGA types have quite literally bought into the cause. Pam Bondi, the attorney-general, holds between $2m and $10m in shares and warrants in Trump Media and Technology Group, which owns Truth Social, the president's social-media network. Ms McMahon sits on the company's board.

No single asset class better illustrates the divide between the financially conservative and the new American right than cryptocurrencies. Mr Trump now has exposure to digital assets himself through the $TRUMP meme coin he launched shortly before his inauguration. Six of the 24 cabinet secretaries and cabinet-level officials own bitcoin or other tokens, including J.D. Vance, the vice-president. This group is in the ascendancy both politically and financially: bitcoin has risen in price by more than 130% in the past year, trouncing returns from traditional assets.

Indeed, two of Mr Trump's most controversial appointments are big digital-asset investors. Robert F. Kennedy junior holds between $1m and $5m in bitcoin. Tulsi Gabbard, the nominee for director of national intelligence, is a crypto omnivore, with $30,000-100,000 in bitcoin and up to $15,000 each in cronos, ethereum and solana, three smaller coins. Although Mr Bessent reports an investment in a bitcoin ETF, it accounts for less than 0.1% of his assets.

The new cabinet's level of crypto enthusiasm outstrips that among the broader American population. According to a survey conducted by the Pew Research Centre, 15% of rich American households own cryptocurrencies, with their popularity skewed to younger investors. Such an unusual level of exposure will surely buttress the administration's support for the industry. Not only is the incoming cabinet ideologically committed to crypto—they have a huge personal stake in its success, too.

Tecnology
Fighting the war in Ukraine on the electromagnetic spectrum

Drone operators and jammers are in a high-tech arms race

Photograph: Sean Sutton/Panos Pictures

FOR SOLDIERS at the front, electromagnetic defences are as vital as air: invisible when present, and disastrous when not. In July Ukrainian troops in southern Donbas found this out the hard way. Abruptly, Russian drones switched frequencies, from standard 700-1,000 megahertz to 400-500 megahertz, blinding Ukraine's electronic-warfare (ew) systems. The drones flew deep behind the lines, cutting off units and making supply routes impassable. Tens of Ukrainian military vehicles were destroyed daily in what Serhii Beskrestnov, a Ukrainian EW specialist, calls a "Russian safari". Only when Ukraine understood what was happening, and secured new EW systems working at 500 megahertz, weeks later, were they able to stabilise the situation.

The war of waves has been pivotal to the wider conflict. A continuous and intense contest between munitions and jammers is driving rapid change, as each side scrambles to find, monitor, occupy and attack increasingly rare gaps in the spectrum where signals can get through. “What you’re seeing in Ukraine is electromagnetic manoeuvre warfare in action,” says Thomas Withington, a fellow at the RUSI think-tank. “Much as land forces are always moving to find that high ground or key crossing, so too are electronic ones.” As jammers become more numerous and more sophisticated, the quest for jam-proof drones becomes ever more urgent.

Russia began its all-out invasion with colossal advantages. It was the world’s EW superpower—if measured by the quantity, might and variety of its systems. It dominated the initial exchanges, jamming much of Ukraine’s military communication. Elon Musk’s Starlink, a secure satellite-communication network, gave a lifeline to Ukraine. Then, in 2023, came the drone revolution. Ukraine pioneered the use of first-person-view (FPV) drones to search, chase and destroy enemy targets with pinpoint accuracy. “Without the proper drone and electronic warfare support, an infantry unit will survive only a few hours on the battlefield,” says Major Dmytro Tolstoluzhsky, an officer in a specialised technology unit of Ukraine’s defence ministry. The task of EW turned to neutralising the drones, loitering munitions and glide bombs that now dominate the skies.

The new war exposed vulnerabilities in Russia’s extremely powerful but bulky EW systems, which became liabilities lying within FPV drone range. They were forced to retreat a full 10-15km away from the front line, diluting their effect. Meanwhile, Ukraine began to make progress expanding its own EW capacity, with local producers scaling up production of trench-level EW systems. Yaroslav Filimonov, the chief executive officer of Kvertus, a Ukrainian company that specialises in EW, says monthly production jumped from 100 devices at the start of 2022 to 1,000 by 2023, and is now up to 5,000. At least 200 companies now work on EW, says Mr Withington.

The basic science of a front-line jammer is not complicated: a cheap metal box with aerials generates electromagnetic noise to block piloting signals or video feeds. Both sides rely heavily on commercially available Chinese components. But beyond this is a constantly evolving, high-stakes technological arms race. Every eight to 12 weeks sees a major change in either EW or drone practice, says Major Tolstoluzhsky. Both sides switch within a wide frequency spectrum from 200 megahertz to 1,000 megahertz, and above. But the “main race” last year, says Andrey Liscovich of the Ukraine Defence Fund, a non-profit which sources non-lethal aid, was a shift in frequencies down from standard GSM bands—those used by mobile phones—to 300 megahertz, making it trickier to find off-the-shelf components.

The result of these proliferating frequencies is vehicles that resemble steampunk porcupines, bristling with half a dozen antennae to protect against different drones, each drawing significant power.

Defenders also have to know where and when to focus their attention. Using a device which spits out a lot of radio waves not only risks electronic fratricide, but also makes the user a potential target. Knowing when to turn it on, and on which frequency, depends on passive sensors which can triangulate radio emissions from the other side to work out their source. The sensors used early in the war, to spot cheaper Chinese-made drones, are no longer as useful. Some of today's sensors are in space: Ukraine is using data from satellites built by HawkEye 360, an American firm.

More common is a spectrum analyser, a small $7,000 box, which picks out the different frequencies broadcasting at any time. That information can then direct your jamming. In theory, spectrum analysers could be strung together to create a giant electronic picket to detect emissions all along the front line. That would cost around $10,000 per kilometre of front, estimates Mr Liscovich, perhaps $10m for the entire stretch—a modest amount. The problem, as with so much else in the war, is supply chains. Only three companies in America and Germany build the devices; turnaround times are eight months.

Both sides are also experimenting with cleverer methods. Mr Filimonov describes Azimuth and Mirage, a pair of products: the first picks up signals within 25km and feeds it to the second, which uses software to generate waveforms on the right frequency. In theory, that frees up the need to carry around several different jammers. But both sides can make disruptive changes. "This is a field of science where everything can be upended in the shortest of time," says Lieutenant Colonel Oleksandr Korobka, who heads an EW unit in Ukraine's 54th brigade.

The top-end Russian drones, for example, have already evolved to include backup piloting systems. They may switch from standard GPS to satellite-led or inertial-navigation systems, which use gyroscopes and accelerometers to work out a drone's real position. They may also use artificial intelligence (AI) or communication with beacons on the ground to move drones to a target or back to base. "In such a case full EW defence is practically impossible," says Colonel Korobka.

The newest challenges are last-mile automation and fibre-optic drones. Last-mile automation avoids most tactical EW shields, which have a range of about 50m, by guiding drones to near a target, and then using AI to visually lock on and strike. Fibre-optic drones, first seen on the battlefield in the spring of 2024, unwind spools of tiny cable as they fly, making them more difficult to manoeuvre but impervious to EW interference. Fibre-optic drones often spearhead attacks, targeting and destroying EW systems first so other radio-piloted drones can follow. Both sides are in the process of ramping up

the technology. Russia, the first-adopter, has a lead. Mr Filimonov says that methods such as stroboscopes—flashing lights to dazzle the drone's cameras—are also being tested.

For now, most drones are still jammable. And Ukraine still has the edge in EW. "They're certainly quicker than the Russians," says Mr Withington. The war has also made them quicker than many Western competitors. Mr Filimonov visited 15 military exhibitions around the world last year. The EW technology he saw was not only pricier—American and European amplifiers are two to three times more expensive than the Chinese ones commonly found in Ukrainian kit—but also obsolete. "These technologies are somewhere in 2021," he says, witheringly. "Everything they are producing is, for the moment, useless on the front line."

Cryptocurrencies are spawning a new generation of private eyes

Their tools are software, and a nose for trouble

Illustration: Alamy/The Economist

FOR THE criminally minded, the allure of cryptocurrencies is easy to grasp. Decentralised online ledgers called blockchains allow digital assets, in the form of "tokens", to be moved without financial institutions monitoring what is happening for signs of money-laundering or other wrongdoing. Chainalysis, a crypto-investigations firm in New York, tallied more than $53bn in suspected crypto-laundering in 2022-23, nearly double its estimate for the previous two years. Nicholas Smart of the Dubai office of Amsterdam-based Crystal Intelligence, another investigator, quips that with blockchains, "Anyone can become a bank."

Then there is the theft of cryptocurrency. As we report in our new podcast series "Scam Inc", so-called pig-butchering cons play on legitimate crypto owners' naivety and emotional vulnerabilities. John Powers, boss of Hudson Intelligence, in New Paltz, New York, says many of his clients have lost tokens worth north of $100,000—and in some cases $1m. They are not alone. This global industry is now worth over $500bn a year worldwide. Crooks, moreover, have surely noted that the potential pool is growing. Token values have soared following America's election of crypto-friendly Donald Trump.

Against this backdrop, specialist firms are developing new forensic software to comb blockchain ledgers in search of stolen digital assets, and to flag possible money-laundering, terrorist financing, and other crimes. The market for such programs is booming. Kroll, an American financial risk and advisory firm, expects revenues from its crypto-sleuthing practice to have exceeded $10m in 2024, roughly double the figure for the previous year.

Making sense of the "data lake" of blockchain ledgers is challenging. Banks, even those in Switzerland, where numbered accounts were invented, are expected to know their account-holders' identities. But blockchains move tokens instantaneously between unique alphanumeric addresses held in digital wallets that can be opened only by private software keys. Though records of the transactions themselves are public, the identities of those behind them are not. Nor is it even clear which addresses are controlled by a given wallet. That opens all sorts of possibilities for money-laundering and illicit payments.

The puzzle of crypto transfers can sometimes, however, be solved by appropriate analytic software. Creators of this are cagey about their tricks, but the frequency and timing of transactions provide clues. An especially fruitful approach is to identify multiple addresses that contribute to a single payment. The private keys to those addresses must be held, or at least controlled, by a single entity. Importantly, as Tom Robinson, chief scientist at Elliptic, a firm in London that develops such software, observes, these "co-spend heuristics" will stand up as evidence in court.

Money laundering and illicit payments are not the only shady activities which transaction patterns can illuminate. The use of "ransomware" is another. Ransomware is software installed illicitly on a computer that then locks valuable data held on it until a crypto payment is made. The proceeds, says Phil Larratt, who was once a financial investigator with Britain's National Crime Agency and now works for Chainalysis, are then typically split about 70-30 between the gang's negotiators and the ransomware's developers.

Mr Larratt says pig-butchering scams involving romance also generate fingerprints. They involve "approval phishing"—fooling lonely hearts into authorising malicious transactions, often with help

from a bogus crypto app. This lets a scammer withdraw the victim's funds. Chainalysis has identified $2.7bn in such fraud since May 2021, passing relevant data to the police. In one case, this allowed the notification of a soon-to-be victim just in time.

Many of Chainalysis's customers are crypto exchanges (places that convert digital assets into conventional currency, and vice versa) seeking to comply with the requirements of the Financial Action Task Force, an intergovernmental body based in Paris. In 2019 this outfit issued rules requiring exchanges in member countries, now numbering 36, to spot and report "sketchy crypto transactions". Similar rules have been put in place elsewhere, too. Red flags include large conversions of digital assets into normal currency despite a high commission, and also the transfer of tokens purchased in cash to multiple exchanges in foreign jurisdictions, especially dodgy ones, like Russia.

"Obfuscation manoeuvres", such as scattering funds into multiple wallets only to reconsolidate them elsewhere, or transfers through several cryptocurrencies, are another tip-off. The best software can now trace assets that have passed through hundreds of wallets. The objective is to identify the funds' arrival in an exchange where they can be seized by a court. Some crypto exchanges even design trading apps to scan users' devices remotely. One warning sign is when multiple accounts are controlled from a single mobile phone, says Azariah Nukajam, compliance boss in Britain for Gemini, an exchange in New York.

Developers of device-scanning software are understandably tight-lipped. But Jeremy Doyle, head of growth for anti-money-laundering analytics at SEON, based in Austin, Texas, and Budapest, says its software assesses things like a phone's number, location, model, storage capacity and how data are entered. Human beings enter data slightly irregularly. Bots tend to be inhumanly precise in such matters.

"Off-chain" work enriches the picture. Many analytics firms send messages feigning interest to fishy exchanges and investment schemes, in order to obtain scammers' crypto addresses. They also monitor online forums where scammers share tips and malicious code. Jeremy Sheridan of FTI Consulting in Washington, DC, says his firm has cracked blockchain investigations with titbits gathered this way. Following social media helps, as well. Mr Smart says he and his colleagues at Crystal Intelligence found a picture of "a box room in a suburb of Beirut" that revealed the QR code of a shady crypto outfit run from the place. Information from an Israeli intelligence service helped his team conclude that the operation had received more than $7m in cash from Hizbullah, a Lebanese terrorist militia.

For all this, the sleuths remain the underdogs. Ironically, the sort of artificial intelligence which might really help cannot be fully applied to crypto investigations. Its complexity means even its programmers

and operators cannot know exactly how it arrives at its conclusions. Those conclusions thus do not stand up as evidence in court. Instead, the software used is “rules-based”, so authorities can see how its conclusions have been drawn. With that unlikely to change, Mr Powers of Hudson Intelligence reckons crypto’s cat-and-mouse game is just getting going.