Here comes cryptocurrency

A quiet revolution in how we buy and sell is under way

S ANANTHANARAYANAN

The rise of digital cash may overturn a world that is already off balance under the effect of the Internet. The Internet, just a curiosity in the 1990s, is now an integral part of everybody's life. But the world still trades using physical money, in the form of real coins, notes or their balances held by trusted bodies called banks, and regulated by governments.

In the world of digital cash, a piece of computer code takes the place of metal, energy or the right of use, which represent the value of money. And transactions in digital cash are recorded not by an intermediary, like a bank, but in an electronic ledger maintained by every computer in the network. The entries are authenticated by links to adjacent entries, in such a way that an alteration would corrupt the record, and transactions are verified by the device of individual "private keys", which ensure authenticity.

The change from cash to Internet banking gave rise to many advantages. But Internet transactions leave a trail of who the buyer was and where she was when she made the purchase. This information could be used, ideally, to help the market position products, or, negatively, to net customers. But the information could also help tag and tail citizens, a violation of privacy.

Digital cash, or cryptocurrency, retains the advantage of dealing through the Internet and, like working with cash, provides anonymity too. The technology, in fact, enables other Internet-based services with the assured identity of the participants, the absence of an intermediary and the immutability of the record. The result may be to redefine the role and function of governments and profound changes in the way corporations, countries and individuals trade and communicate.

The Princeton University Press, Princeton and Oxford, has brought out *Digital Cash: The Unknown History of the Anarchists, Utopians and Technologists Who Build Cryptocurrency*, a book by Finn Brunton, which describes exactly what the title says. Over 208 pages, followed by 35 pages of notes and bibliography, Brunton, assistant professor in the department of media, culture and communication, New York University, takes the reader though the conceptual bases, the cultural progression, of barter, coinage, the banknote, codes and devices to protect cyber transactions, the criteria, priorities and controls.

The first things that we ask for in any form of cash, or tokens of money, Brunton says, is that you know it is genuine, and that it has value, which it will not lose. The earliest coins were of precious metals, whose value was related to the labour it took to mine them, their authenticity could be tested and the market could not be flooded with duplicates. It was the same when kings and states struck coins; they represented value and were difficult or expensive to counterfeit. Bills of exchange replaced physical money and enabled trade based on the chain of trust reposed in those who signed the bills. And banknotes bore a trusted signature to work as a vehicle for trade among strangers and contained devices to prevent duplication. The demand placed on the instrument, Brunton says, is that it be "easily recognisable, but impossible to duplicate."

Moving on to the digital age, Brunton examines the issues that arise when messages need to be kept secret from eavesdroppers, yet recognised as genuine by the proper recipient. He describes the ciphers used by spies during World War II. Messages were scrambled based on a predetermined key and were secure for some time, but not for longer, as codes could be broken. Fresh keys had to be frequently exchanged, and this was a challenge and vulnerability. Brunton recognises these keys, which need to be shared, as symmetrical keys.

A solution would be a pair of asymmetrical keys, where the sender uses one key to code the message and the receiver another key to decode the message. This was a solution that many had been looking for, Brunton explains, and it was found at about the same time by more than one researcher — in the form of the "public key and private key algorithm".

It consists of a mathematical procedure of using both keys at the time of encryption, or the coding of the message, in such a way that it can be decoded only with the help of the key known as the public key. A receiver, who decodes the message with the sender's public key, knows for certain who it was that sent the messages, as the message cannot be decoded by any other public key. The message can be opened by an eavesdropper too, but there is no way the private key, which was used to code the message, can be worked out. The message, therefore, cannot be altered and coded again by adversaries.

Similarly, a message that has to be kept secret can be coded with the recipient's public key. Now, this message can be decoded only by the private key of the person whose public key was used for coding. Eavesdroppers can hence intercept the message, but they cannot read what it says — it stays secret. If a message is coded by a private key and then the receiver's public key, it is both digitally signed as well as secret.

This device of the "public-private keys" is the basis of digital signatures and much of e-commerce. But cryptocurrency goes one further. An algorithmically processed text is itself the currency, of the medium of exchange of value, generated as representing the computational work done to create it. Transactions and balances in cryptocurrency are not recorded, as in the case of normal currency, in the ledger of a bank, but in a series of transaction records, known as blocks, in the computers in the network of all the users of the system. Each block is linked to the preceding block with the help of codes derived from the contents of the blocks, in such a manner that any alteration of a block, or the details of a transaction, would disrupt that series, known as the blockchain.

FINN BRUNTON
DIGITAL CASH
THE UNKNOWN HISTORY OF THE ANARCHISTS, UTOPIANS, AND TECHNOLOGISTS WHO CREATED CRYPTOCURRENCY

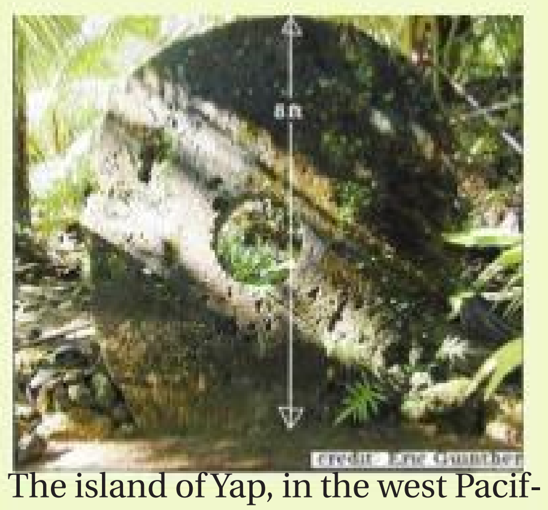
The system thus has no central administrator, like a bank, which maintains the accounts, and the network records all transactions and transfer of ownership of cryptocurrency and prevents the reuse of a token that has been transferred. As every computer on the network, which may have millions of nodes, has a copy of the blockchain, the network is practically incorruptible.

The system has been operational for some years. Bitcoin (short for Binary Digit coin) is the most popular cryptocurrency in use, but there are others. And the blockchain technology also works for recording transactions like contracts, for medical consultations and many others; it could even be government records, where the requirement is confidentiality, reliability and permanence.

Brunton's book is an important record of concepts and the players that have contributed to what may represent a whole new phase of civilisation, which has been fashioned, so far, based on transactions that are supervised and assured by a central authority.

The writer can be contacted at
response@simplescience.in

Stone money



The island of Yap, in the west Pacific Ocean, has an ancient monetary system based on a ledger maintained by the community. The actual cash consists of large stone discs, difficult to counterfeit, as it takes work to fashion them, and difficult to move. During a transaction, the stone does not change hands, only the ownership of the stone, or part of it, passes from the buyer, of the commodity traded, to the seller. The accounting is in the form of an announcement made to the inhabitants of the island, and cannot be repudiated or changed, and the stone or the part that has been spent cannot be used again by the one who has spent it.

PLUS POINTS

Marmoset at risk

A completely new species of marmoset monkey that was discovered just weeks ago, is now believed to be at significant risk due to the fires, which continue to burn through the Amazon rainforest.

The *Mico munduruku* marmoset is unusual because of its white tail and hands. Typically the creature has black tails. It is only believed to live within an area approximately 55,000 sq km within Pará State in Brazil's southwest. The creature was discovered in August by Rodrigo Costa Araújo and his colleagues at the National Institute of Amazonian Research and the Federal University of Amazonas in Brazil.

The catastrophic blazes have devastated the landscape on an unprecedented scale. Combined with illegal logging, agricultural expansion and new energy and infrastructure projects, the natural habitat of countless creatures is rapidly being permanently destroyed. In some cases the accelerated destruction is taking place just as we are becoming aware of what we are losing.

One fire runs directly through the newly-found marmoset's range, Araújo told charity Flora & Fauna International, citing Nasa satellite data. "Once these forests are gone, the marmosets will be gone too," he said. "And this year's fires are burning much more habitat of all southern Amazonian marmosets than in past years."

Araújo added the setting of the fires, which have swept through swathes of the Brazilian Amazon this year, was "politically motivated". He said this was not a year of reduced rainfall and drier conditions, which increase fire risks. The prices of soy crops and beef had not drastically risen to prompt farmers to clear more agricultural land, he added.

"The obvious conclusion is that the 2019 fires are politically motivated, with farmers supporting the agenda of the president against environment and biodiversity conservation. And the president is in turn supporting these people on the ground," he said.

Araújo said Brazil's right wing president Jair Bolsonaro had "been systematically dismantling the country's framework for monitoring and preventing deforestation, cutting the budget of the national environment agency, refusing absolutely vital international support.. and proposing the relaxation of environmental."

However, he added that the discovery of the new marmoset could have a positive impact by causing a review to be held into the construction of major hydroelectric power plants, which are all within the species' range. He said, "This region has hardly been studied and its biodiversity is poorly known, so having a new primate species described from there clearly demonstrates that we are destroying the habitat of many other, still undiscovered species."

The independent

Helping make sense of the universe

This year's Nobel Prize in Physics has been awarded for two seminal breakthroughs — evidence for the Big Bang and a way to find exoplanets

Nobel Prize winners in physics, from left, James Peebles in Princeton,US, Didier Queloz in London and Michel Mayor in Madrid.

ROBERT T FISHER

Did the universe really begin with a Big Bang? And if so, is there evidence? Are there planets around other stars? Can they support life? The 2019 Nobel Prize in Physics goes to three scientists who have provided deep insights into all of these questions.

James Peebles, an emeritus professor of physics at Princeton University, won half the prize for a body of work he completed since the 1960s, when he and a team of physicists at Princeton attempted to detect the remnant radiation of the dense, hot ball of gas at the beginning of the universe — the Big Bang.

The other half went to Michel Mayor, an emeritus professor of physics from the University of Geneva, together with Didier Queloz, also a Swiss astrophysicist at the University of Geneva and the University of Cambridge. Both made breakthroughs with the discovery of the first planets orbiting other stars, also known as exoplanets, beyond our solar system.

I am an astrophysicist and was delighted to hear of this year's Nobel recipients, who had a profound impact on scientists' understanding of the universe. A lot of my own work on exploding stars is guided by theories describing the structure of the universe that Peebles himself laid down.

In fact, one might say that Peebles, of all this year's Nobel winners, is the biggest star of the real "Big Bang Theory."

The real Big Bang Theory

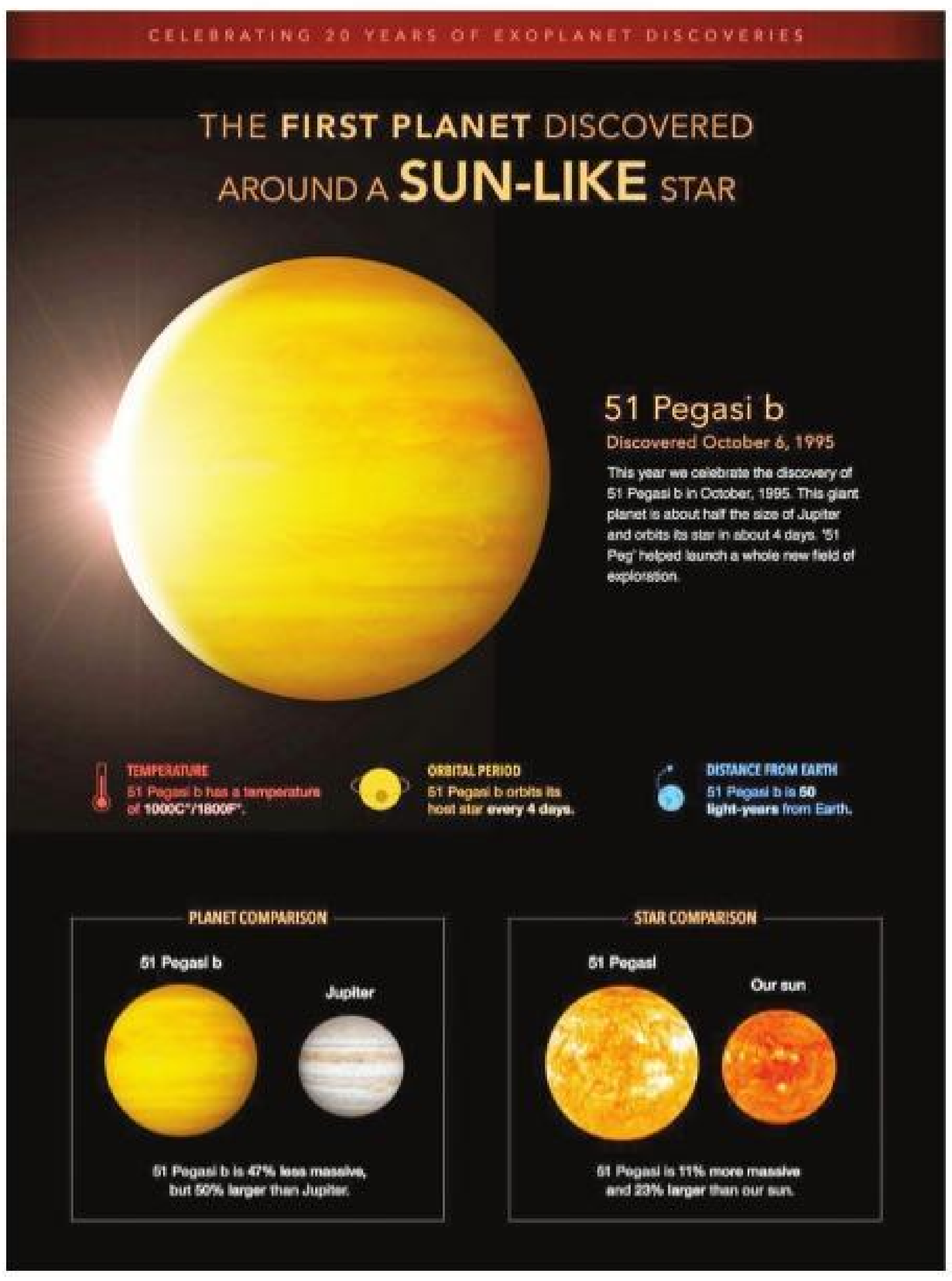
As Peebles and his Princeton team rushed to complete their discovery in 1964, they were scooped by two young scientists at nearby Bell Labs, Arno Penzias and Robert Wilson. The remaining radiation from the Big Bang was predicted to be microwave energy, in much the same form used by countertop ovens.

It was a serendipitous finding because Penzias and Wilson had constructed an antenna to detect this microwave radiation, which was used in satellite communications. But they were mystified by a persistent source of noise in their measurements, like the fuzz of a radio tuned between stations.

Penzias and Wilson talked to Peebles and his colleagues and learned that this static they were hearing was the radiation left over from the Big Bang itself. Penzias and Wilson won the Nobel Prize in 1978 for their discovery, though Peebles and his team provided the crucial interpretation.

Peebles has also made decades of pivotal contributions to the study of the matter, which pervades the cosmos but is invisible to telescopes, known as dark matter, and the equally mysterious energy of empty space, known as dark energy. He has done foundational work on the formation of galaxies, as well as to how the Big Bang gave rise to the first elements — hydrogen, helium, lithium — on the periodic table.

Finding planets beyond our solar system



CELEBRATING 20 YEARS OF EXOPLANET DISCOVERIES
THE FIRST PLANET DISCOVERED AROUND A SUN-LIKE STAR
51 Pegasi b
Discovered October 6, 1995
This year we celebrate the discovery of 51 Pegasi b in October, 1995. This giant planet is about half the size of Jupiter and orbits its star in about 4 days. '51 Peg' helped launch a whole new field of exploration.
TEMPERATURE
51 Pegasi b has a temperature of 1000C°/1800F°.
ORBITAL PERIOD
51 Pegasi b orbits its host star every 4 days.
DISTANCE FROM EARTH
51 Pegasi b is 50 light-years from Earth.
PLANET COMPARISON
51 Pegasi b
Jupiter
51 Pegasi b is 47% less massive, but 50% larger than Jupiter.
STAR COMPARISON
51 Pegasi
Our sun
51 Pegasi is 11% more massive and 23% larger than our sun.

For their Nobel Prize-winning work, Mayor and Queloz carried out a survey of nearby stars using a custom-built instrument. Using this instrument, they could detect the wobble of a star — a sign that it is being tugged by the gravity of an orbiting exoplanet.

In 1995, in a landmark discovery published in the journal Nature, they found a star in the constellation Pegasus rapidly wobbling across the sky, in response to an unseen planet with half the mass of Jupiter. This exoplanet, dubbed 51 Pegasi b, orbits close to its central star, well within the orbit of Mercury in our own solar system, and completes one full orbit in just four days.

This surprising discovery of a "hot Jupiter," quite unlike any planet in our own solar system, excited the astrophysical community and inspired many other research groups, including the Kepler space telescope team, to search for exoplanets.

These groups are using both the same wobble detection method as well as new methods, such as looking for light dips caused by exoplanets passing over nearby stars. Thanks to these research efforts, more than 4,000 exoplanets have now been discovered.

The writer is associate professor of physics, University of Massachusetts Dartmouth, US. This article first appeared on www.theconversation.com

Smart design

Emphasising on the greater penetration of electric vehicles on roads, the Indian Institute of Technology- Guwahati has recently announced the development of an artificial intelligence-assisted engineering system design tool. Titled "Smart-Engineer", the tool has been built by a team comprising of PhD and Masters students of the premier institution.

"Smart-Engineer", built by the e-mobility lab at IIT-G seeks to address one of the primary hurdles in indigenising the EV technology, which is the lack of trained human resources in engineering design and system integration. The current version of Smart-Engineer is able to address the fundamentals involved in the design of induction motors. "The early results are promising, and we now intend to expand the capability of Smart-Engineer to include the finer aspects of motor design", said a statement from IIT-G.

Smart-Engineer will enable companies to store and maintain the collective knowledge of expert engineers, which in turn can preserve and promote further theoretical and practical advancements in design thinking/ philosophy. Eventually, the collective knowledge and wisdom will be used and further enriched by the next generation of engineers, it added.

Nava Thakuria