

RESEARH ON CRYPTO CURRENCY

A cryptocurrency (or crypto currency) is a digital asset designed to work as a medium of exchange wherein individual coin ownership records are stored in a digital ledger or computerized database using strong cryptography to secure transaction record entries, to control the creation of additional digital coin records, and to verify the transfer of coin ownership. It typically does not exist in physical form (like paper money) and is typically not issued by a central authority. Some cryptocurrencies use decentralized control as opposed to centralized digital currency and central banking systems. When a cryptocurrency is minted or created prior to issuance or held on a centralized exchange, it is generally considered centralized. When implemented with decentralized control, each cryptocurrency works through distributed ledger technology, typically a blockchain, that serves as a public financial transaction database.

Bitcoin, first released as open-source software in 2009, is the first decentralized cryptocurrency. Since the release of bitcoin, over 6,000 altcoins (alternative variants of bitcoin, or other cryptocurrencies) have been created.

IMPORTANCE OF CRYPTO CURRENCY

According to Jan Lansky, a cryptocurrency is a system that meets six conditions:

1. The system does not require a central authority, its state is maintained through distributed consensus.
2. The system keeps an overview of cryptocurrency units and their ownership.
3. The system defines whether new cryptocurrency units can be created. If new cryptocurrency units can be created, the system defines the circumstances of their origin and how to determine the ownership of these new units.
4. Ownership of cryptocurrency units can be proved exclusively cryptographically.
5. The system allows transactions to be performed in which ownership of the cryptographic units is changed. A transaction statement can only be issued by an entity proving the current ownership of these units.
6. If two different instructions for changing the ownership of the same cryptographic units are simultaneously entered, the system performs at most one of them.

OTHER TERMS IN CRYPTO CURRENCY

Altcoin

The term altcoin has various similar definitions. Stephanie Yang of The Wall Street Journal defined altcoins as "alternative digital currencies," while Paul Vigna, also of The Wall Street Journal, described altcoins as alternative versions of bitcoin. Aaron Hankins of MarketWatch refers to any cryptocurrencies other than bitcoin as altcoins.

Crypto token

A blockchain account can provide functions other than making payments, for example in decentralized applications or smart contracts. In this case, the units or coins are sometimes referred to as crypto tokens (or cryptotokens).

THE HISTORY OF CRYPTO CURRENCY

In 1983, the American cryptographer David Chaum conceived an anonymous cryptographic electronic money called ecash. Later, in 1995, he implemented it through Digicash, an early form of cryptographic electronic payments which required user software in order to withdraw notes from a bank and designate specific encrypted keys before it can be sent to a recipient. This allowed the digital currency to be untraceable by the issuing bank, the government, or any third party.

In 1996, the National Security Agency published a paper entitled How to Make a Mint: the Cryptography of Anonymous Electronic Cash, describing a Cryptocurrency system, first publishing it in an MIT mailing list and later in 1997, in The American Law Review (Vol. 46, Issue 4).

In 1998, Wei Dai published a description of "b-money", characterized as an anonymous, distributed electronic cash system. Shortly thereafter, Nick Szabo described bit gold. Like bitcoin and other cryptocurrencies that would follow it, bit gold (not to be confused with the later gold-based exchange, BitGold) was described as an electronic currency system which required users to complete a proof of work function with solutions being cryptographically put together and published.

The first decentralized cryptocurrency, bitcoin, was created in 2009 by presumably pseudonymous developer Satoshi Nakamoto. It used SHA-256, a cryptographic hash function, as its proof-of-work scheme. In April 2011, Namecoin was created as an attempt at forming a decentralized DNS, which would make internet censorship very difficult. Soon after, in October 2011, Litecoin was released. It was the first successful cryptocurrency to use scrypt as its hash function instead of SHA-256. Another notable cryptocurrency, Peercoin was the first to use a proof-of-work/proof-of-stake hybrid.

On 6 August 2014, the UK announced its Treasury had been commissioned to do a study of cryptocurrencies, and what role, if any, they can play in the UK economy. The study was also to report on whether regulation should be considered.

THE ARCHITECTURE OF CRYPTO CURRENCY

Decentralized cryptocurrency is produced by the entire cryptocurrency system collectively, at a rate which is defined when the system is created and which is publicly known. In centralized banking and economic systems such as the Federal Reserve System, corporate boards or governments control the supply of currency by printing units of fiat money or demanding additions to digital banking ledgers. In the case of decentralized cryptocurrency, companies or

governments cannot produce new units, and have not so far provided backing for other firms, banks or corporate entities which hold asset value measured in it. The underlying technical system upon which decentralized cryptocurrencies are based was created by the group or individual known as Satoshi Nakamoto.

As of May 2018, over 1,800 cryptocurrency specifications existed. Within a cryptocurrency system, the safety, integrity and balance of ledgers is maintained by a community of mutually distrustful parties referred to as miners: who use their computers to help validate and timestamp transactions, adding them to the ledger in accordance with a particular timestamping scheme.

Most cryptocurrencies are designed to gradually decrease production of that currency, placing a cap on the total amount of that currency that will ever be in circulation. Compared with ordinary currencies held by financial institutions or kept as cash on hand, cryptocurrencies can be more difficult for seizure by law enforcement. This difficulty is derived from leveraging cryptographic technologies.

Blockchain

The validity of each cryptocurrency's coins is provided by a blockchain. A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data. By design, blockchains are inherently resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority.

Blockchains are secure by design and are an example of a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been achieved with a blockchain. The public nature of the blockchain ledger protects the integrity of whatever is being transacted since no one entity owns the database. The added work required to solve the encryption in a proof-of-stake system ensures that the public ledger is not modified at random, thus solving the double-spending problem without the need of a trusted authority or central server to administer the database, assuming no 51% attack (that has worked against several cryptocurrencies).

Timestamping

Cryptocurrencies use various timestamping schemes to "prove" the validity of transactions added to the blockchain ledger without the need for a trusted third party. The first timestamping scheme invented was the proof-of-work scheme. The most widely used proof-of-work schemes are based on SHA-256 and scrypt. Some other hashing algorithms that are used for proof-of-work include CryptoNight, Blake, SHA-3, and X11.

The proof-of-stake is a method of securing a cryptocurrency network and achieving distributed consensus through requesting users to show ownership of a certain amount of currency. It is different from proof-of-work systems that run difficult hashing algorithms to validate electronic transactions. The scheme is largely dependent on the coin, and there's currently no standard form of it. Some cryptocurrencies use a combined proof-of-work and proof-of-stake scheme.

Mining

In cryptocurrency networks, mining is a validation of transactions. For this effort, successful miners obtain new cryptocurrency as a reward. The reward decreases transaction fees by creating a complementary incentive to contribute to the processing power of the network. The rate of generating hashes, which validate any transaction, has been increased by the use of specialized machines such as FPGAs and ASICs running complex hashing algorithms like SHA-256 and Scrypt.[citation needed] This arms race for cheaper-yet-efficient machines has existed since the day the first cryptocurrency, bitcoin, was introduced in 2009. With more people venturing into the world of virtual currency, generating hashes for this validation has become far more complex over the years, with miners having to invest large sums of money on employing multiple high performance ASICs. Thus the value of the currency obtained for finding a hash often does not justify the amount of money spent on setting up the machines, the cooling facilities to overcome the heat they produce, and the electricity required to run them. As of July 2019, bitcoin's electricity consumption is estimated to about 7 gigawatts, 0.2% of the global total, or equivalent to that of Switzerland.

Some miners pool resources, sharing their processing power over a network to split the reward equally, according to the amount of work they contributed to the probability of finding a block. A "share" is awarded to members of the mining pool who present a valid partial proof-of-work. As of February 2018, the Chinese Government halted trading of virtual currency, banned initial coin offerings and shut down mining. Some Chinese miners have since relocated to Canada. One company is operating data centers for mining operations at Canadian oil and gas field sites, due to low gas prices. In June 2018, Hydro Quebec proposed to the provincial government to allocate 500 MW to crypto companies for mining. According to a February 2018 report from Fortune, Iceland has become a haven for cryptocurrency miners in part because of its cheap electricity. In March 2018, a town in Upstate New York put an 18-month moratorium on all cryptocurrency mining in an effort to preserve natural resources and the "character and direction" of the city.

GPU price rise

An increase in cryptocurrency mining increased the demand for graphics cards (GPU) in 2017. (The computing power of GPUs makes them well-suited to generating hashes.) Popular favorites of cryptocurrency miners such as Nvidia's GTX 1060 and GTX 1070 graphics cards, as well as AMD's RX 570 and RX 580 GPUs, doubled or tripled in price – or were out of stock. A GTX 1070 Ti which was released at a price of \$450 sold for as much as \$1100. Another popular card GTX 1060's 6 GB model was released at an MSRP of \$250, sold for almost \$500. RX 570 and RX 580

cards from AMD were out of stock for almost a year. Miners regularly buy up the entire stock of new GPU's as soon as they are available. Nvidia has asked retailers to do what they can when it comes to selling GPUs to gamers instead of miners. "Gamers come first for Nvidia," said Boris Böhles, PR manager for Nvidia in the German region.

Wallets

An example paper printable bitcoin wallet consisting of one bitcoin address for receiving and the corresponding private key for spending. A cryptocurrency wallet stores the public and private "keys" or "addresses" which can be used to receive or spend the cryptocurrency. With the private key, it is possible to write in the public ledger, effectively spending the associated cryptocurrency. With the public key, it is possible for others to send currency to the wallet.

Anonymity

Bitcoin is pseudonymous rather than anonymous in that the cryptocurrency within a wallet is not tied to people, but rather to one or more specific keys (or "addresses"). Thereby, bitcoin owners are not identifiable, but all transactions are publicly available in the blockchain. Still, cryptocurrency exchanges are often required by law to collect the personal information of their users.

Additions such as Zerocoin, Zerocash and CryptoNote have been suggested, which would allow for additional anonymity and fungibility.

Fungibility

Most cryptocurrency tokens are fungible and interchangeable. However, unique non-fungible tokens also exist. Such tokens can serve as assets in games like CryptoKitties.

THE ECONOMY OF CRYPTO CURRENCY

Cryptocurrencies are used primarily outside existing banking and governmental institutions and are exchanged over the Internet.

Block rewards

Proof-of-work cryptocurrencies, such as bitcoin, offer block rewards incentives for miners. There has been an implicit belief that whether miners are paid by block rewards or transaction fees does not affect the security of the blockchain, but a study suggests that this may not be the case under certain circumstances.

The rewards paid to miners increase the supply of the cryptocurrency. By making sure that verifying transactions is a costly business, the integrity of the network can be preserved as long as benevolent nodes control a majority of computing power. The verification algorithm requires a lot of processing power, and thus electricity in order to make verification costly enough to accurately validate public blockchain. Not only do miners have to factor in the costs associated with expensive equipment necessary to stand a chance of solving a hash problem, they further must consider the significant amount of electrical power in search of the solution. Generally, the block rewards outweigh electricity and equipment costs, but this may not always be the case.

The current value, not the long-term value, of the cryptocurrency supports the reward scheme to incentivize miners to engage in costly mining activities. Some sources claim that the current bitcoin design is very inefficient, generating a welfare loss of 1.4% relative to an efficient cash system. The main source for this inefficiency is the large mining cost, which is estimated to be 360 Million USD per year. This translates into users being willing to accept a cash system with an inflation rate of 230% before being better off using bitcoin as a means of payment. However, the efficiency of the bitcoin system can be significantly improved by optimizing the rate of coin creation and minimizing transaction fees. Another potential improvement is to eliminate inefficient mining activities by changing the consensus protocol altogether.

Transaction fees

Transaction fees for cryptocurrency depend mainly on the supply of network capacity at the time, versus the demand from the currency holder for a faster transaction. The currency holder can choose a specific transaction fee, while network entities process transactions in order of highest offered fee to lowest. Cryptocurrency exchanges can simplify the process for currency holders by offering priority alternatives and thereby determine which fee will likely cause the transaction to be processed in the requested time.

For ether, transaction fees differ by computational complexity, bandwidth use, and storage needs, while bitcoin transaction fees differ by transaction size and whether the transaction uses SegWit. In September 2018, the median transaction fee for ether corresponded to \$0.017, while for bitcoin it corresponded to \$0.55. Some cryptocurrencies have no transaction fees, and instead rely on client-side proof-of-work as the transaction prioritization and anti-spam mechanism.

Exchanges

Cryptocurrency exchanges allow customers to trade cryptocurrencies for other assets, such as conventional fiat money, or to trade between different digital currencies.

Atomic swaps

Atomic swaps are a mechanism where one cryptocurrency can be exchanged directly for another cryptocurrency, without the need for a trusted third party such as an exchange.

ATMs

Bitcoin ATM

Jordan Kelley, founder of Robocoin, launched the first bitcoin ATM in the United States on 20 February 2014. The kiosk installed in Austin, Texas is similar to bank ATMs but has scanners to read government-issued identification such as a driver's license or a passport to confirm users' identities.

Initial coin offerings

An initial coin offering (ICO) is a controversial means of raising funds for a new cryptocurrency venture. An ICO may be used by startups with the intention of avoiding regulation. However, securities regulators in many jurisdictions, including in the U.S., and Canada have indicated that

if a coin or token is an "investment contract" (e.g., under the Howey test, i.e., an investment of money with a reasonable expectation of profit based significantly on the entrepreneurial or managerial efforts of others), it is a security and is subject to securities regulation. In an ICO campaign, a percentage of the cryptocurrency (usually in the form of "tokens") is sold to early backers of the project in exchange for legal tender or other cryptocurrencies, often bitcoin or ether. According to PricewaterhouseCoopers, four of the 10 biggest proposed initial coin offerings have used Switzerland as a base, where they are frequently registered as non-profit foundations. The Swiss regulatory agency FINMA stated that it would take a "balanced approach" to ICO projects and would allow "legitimate innovators to navigate the regulatory landscape and so launch their projects in a way consistent with national laws protecting investors and the integrity of the financial system." In response to numerous requests by industry representatives, a legislative ICO working group began to issue legal guidelines in 2018, which are intended to remove uncertainty from cryptocurrency offerings and to establish sustainable business practices.

THE LEGALITY OF CRYPTO CURRENCY

The legal status of cryptocurrencies varies substantially from country to country and is still undefined or changing in many of them. While some countries have explicitly allowed their use and trade, others have banned or restricted it. According to the Library of Congress, an "absolute ban" on trading or using cryptocurrencies applies in eight countries: Algeria, Bolivia, Egypt, Iraq, Morocco, Nepal, Pakistan, and the United Arab Emirates. An "implicit ban" applies in another 15 countries, which include Bahrain, Bangladesh, China, Colombia, the Dominican Republic, Indonesia, Iran, Kuwait, Lesotho, Lithuania, Macau, Oman, Qatar, Saudi Arabia and Taiwan. In the United States and Canada, state and provincial securities regulators, coordinated through the North American Securities Administrators Association, are investigating "bitcoin scams" and ICOs in 40 jurisdictions. Various government agencies, departments, and courts have classified bitcoin differently. China Central Bank banned the handling of bitcoins by financial institutions in China in early 2014.

In Russia, though cryptocurrencies are legal, it is illegal to actually purchase goods with any currency other than the Russian ruble. Regulations and bans that apply to bitcoin probably extend to similar cryptocurrency systems. Cryptocurrencies are a potential tool to evade economic sanctions for example against Russia, Iran, or Venezuela. Russia also secretly supported Venezuela with the creation of the petro (El Petro), a national cryptocurrency initiated by the Maduro government to obtain valuable oil revenues by circumventing US sanctions.

In August 2018, the Bank of Thailand announced its plans to create its own cryptocurrency, the Central Bank Digital Currency (CBDC).

Advertising bans

Cryptocurrency advertisements were temporarily banned on Facebook, Google, Twitter, Bing, Snapchat, LinkedIn and MailChimp. Chinese internet platforms Baidu, Tencent, and Weibo have

also prohibited bitcoin advertisements. The Japanese platform Line and the Russian platform Yandex have similar prohibitions.

U.S. tax status

On 25 March 2014, the United States Internal Revenue Service (IRS) ruled that bitcoin will be treated as property for tax purposes. This means bitcoin will be subject to capital gains tax. In a paper published by researchers from Oxford and Warwick, it was shown that bitcoin has some characteristics more like the precious metals market than traditional currencies, hence in agreement with the IRS decision even if based on different reasons. In July 2019, the IRS started sending letters to cryptocurrency owners warning them to amend their returns and pay taxes.

The legal concern of an unregulated global economy

As the popularity of and demand for online currencies has increased since the inception of bitcoin in 2009, so have concerns that such an unregulated person to person global economy that cryptocurrencies offer may become a threat to society. Concerns abound that altcoins may become tools for anonymous web criminals. Cryptocurrency networks display a lack of regulation that has been criticized as enabling criminals who seek to evade taxes and launder money.

Transactions that occur through the use and exchange of these altcoins are independent from formal banking systems, and therefore can make tax evasion simpler for individuals. Since charting taxable income is based upon what a recipient reports to the revenue service, it becomes extremely difficult to account for transactions made using existing cryptocurrencies, a mode of exchange that is complex and difficult to track. Systems of anonymity that most cryptocurrencies offer can also serve as a simpler means to launder money. Rather than laundering money through an intricate net of financial actors and offshore bank accounts, laundering money through altcoins can be achieved through anonymous transactions.

Loss, theft, and fraud

In February 2014 the world's largest bitcoin exchange, Mt. Gox, declared bankruptcy. The company stated that it had lost nearly \$473 million of their customers' bitcoins likely due to theft. This was equivalent to approximately 750,000 bitcoins, or about 7% of all the bitcoins in existence. The price of a bitcoin fell from a high of about \$1,160 in December to under \$400 in February. Two members of the Silk Road Task Force—a multi-agency federal task force that carried out the U.S. investigation of Silk Road—seized bitcoins for their own use in the course of the investigation. DEA agent Carl Mark Force IV, who attempted to extort Silk Road founder Ross Ulbricht ("Dread Pirate Roberts"), pleaded guilty to money laundering, obstruction of justice, and extortion under color of official right, and was sentenced to 6.5 years in federal prison. U.S. Secret Service agent Shaun Bridges pleaded guilty to crimes relating to his diversion of \$800,000 worth of bitcoins to his personal account during the investigation, and also separately pleaded guilty to

money laundering in connection with another cryptocurrency theft; he was sentenced to nearly eight years in federal prison.

Homero Josh Garza, who founded the cryptocurrency startups GAW Miners and ZenMiner in 2014, acknowledged in a plea agreement that the companies were part of a pyramid scheme, and pleaded guilty to wire fraud in 2015. The U.S. Securities and Exchange Commission separately brought a civil enforcement action against Garza, who was eventually ordered to pay a judgment of \$9.1 million plus \$700,000 in interest. The SEC's complaint stated that Garza, through his companies, had fraudulently sold "investment contracts representing shares in the profits they claimed would be generated" from mining.

On 21 November 2017, the Tether cryptocurrency announced they were hacked, losing \$31 million in USDT from their primary wallet. The company has 'tagged' the stolen currency, hoping to 'lock' them in the hacker's wallet (making them unspendable). Tether indicates that it is building a new core for its primary wallet in response to the attack in order to prevent the stolen coins from being used.

In May 2018, Bitcoin Gold (and two other cryptocurrencies) were hit by a successful 51% hashing attack by an unknown actor, in which exchanges lost estimated \$18m. In June 2018, Korean exchange Coinrail was hacked, losing US\$37 million worth of altcoin. Fear surrounding the hack was blamed for a \$42 billion cryptocurrency market selloff. On 9 July 2018 the exchange Bancor had \$23.5 million in cryptocurrency stolen.

The French regulator Autorité des marchés financiers (AMF) lists 15 websites of companies that solicit investment in cryptocurrency without being authorised to do so in France.

Darknet markets

Properties of cryptocurrencies gave them popularity in applications such as a safe haven in banking crises and means of payment, which also led to the cryptocurrency use in controversial settings in the form of online black markets, such as Silk Road. The original Silk Road was shut down in October 2013 and there have been two more versions in use since then. In the year following the initial shutdown of Silk Road, the number of prominent dark markets increased from four to twelve, while the amount of drug listings increased from 18,000 to 32,000.

Darknet markets present challenges in regard to legality. Cryptocurrency used in dark markets are not clearly or legally classified in almost all parts of the world. In the U.S., bitcoins are labelled as "virtual assets". This type of ambiguous classification puts pressure on law enforcement agencies around the world to adapt to the shifting drug trade of dark markets.

THE RECEPTION OF CRYPTO CURRENCY

Cryptocurrencies have been compared to Ponzi schemes, pyramid schemes and economic bubbles, such as housing market bubbles. Howard Marks of Oaktree Capital Management stated in 2017 that digital currencies were "nothing but an unfounded fad (or perhaps even a pyramid scheme), based on a willingness to ascribe value to something that has little or none beyond what

people will pay for it", and compared them to the tulip mania (1637), South Sea Bubble (1720), and dot-com bubble (1999). The New Yorker has explained the debate based on interviews with blockchain founders in an article about the "argument over whether Bitcoin, Ethereum, and the blockchain are transforming the world".

While cryptocurrencies are digital currencies that are managed through advanced encryption techniques, many governments have taken a cautious approach toward them, fearing their lack of central control and the effects they could have on financial security.[88] Regulators in several countries have warned against cryptocurrency and some have taken concrete regulatory measures to dissuade users. Additionally, many banks do not offer services for cryptocurrencies and can refuse to offer services to virtual-currency companies. Gareth Murphy, a senior central banking officer has stated "widespread use [of cryptocurrency] would also make it more difficult for statistical agencies to gather data on economic activity, which are used by governments to steer the economy". He cautioned that virtual currencies pose a new challenge to central banks' control over the important functions of monetary and exchange rate policy. While traditional financial products have strong consumer protections in place, there is no intermediary with the power to limit consumer losses if bitcoins are lost or stolen. One of the features cryptocurrency lacks in comparison to credit cards, for example, is consumer protection against fraud, such as chargebacks.

Bitcoin has been criticized by its opponents for the amount of energy that goes into its proof-of-work cryptocurrency mining; cryptocurrency proponents claim it is important to compare the energy spent to the consumption of the traditional financial system.

There are also purely technical elements to consider. For example, technological advancement in cryptocurrencies such as bitcoin result in high up-front costs to miners in the form of specialized hardware and software. Cryptocurrency transactions are normally irreversible after a number of blocks confirm the transaction. Additionally, cryptocurrency private keys can be permanently lost from local storage due to malware, data loss or the destruction of the physical media. This prevents the cryptocurrency from being spent, resulting in its effective removal from the markets. The cryptocurrency community refers to pre-mining, hidden launches, ICO or extreme rewards for the altcoin founders as a deceptive practice. It can also be used as an inherent part of a cryptocurrency's design. Pre-mining means currency is generated by the currency's founders prior to being released to the public.

Paul Krugman, winner of the Nobel Memorial Prize in Economic Sciences, has repeated numerous times that it is a bubble that will not last[99] and links it to Tulip mania. American business magnate Warren Buffett thinks that cryptocurrency will come to a bad ending. In October 2017, BlackRock CEO Laurence D. Fink called bitcoin an 'index of money laundering'. "Bitcoin just shows you how much demand for money laundering there is in the world," he said.

Academic studies

In September 2015, the establishment of the peer-reviewed academic journal Ledger (ISSN 2379-5980) was announced. It covers studies of cryptocurrencies and related technologies, and is published by the University of Pittsburgh.

The journal encourages authors to digitally sign a file hash of submitted papers, which will then be timestamped into the bitcoin blockchain. Authors are also asked to include a personal bitcoin address in the first page of their papers.

Aid agencies

A number of aid agencies have started accepting donations in cryptocurrencies, including the American Red Cross, UNICEF[106] , and the UN World Food Program. Cryptocurrencies make tracking donations easier and have the potential to allow donors to see how their money is used (financial transparency).

Christopher Fabian, principal adviser at UNICEF Innovation said that UNICEF would uphold existing donor protocols, meaning that those making donations online would have to pass rigorous checks before they were allowed to deposit funds to UNICEF.

THE FUTURE OF CRYPTO CURRENCY

Some economic analysts predict a big change in crypto is forthcoming as institutional money enters the market. Moreover, there is the possibility that crypto will be floated on the Nasdaq, which would further add credibility to blockchain and its uses as an alternative to conventional currencies. Some predict that all that crypto needs is a verified exchange traded fund (ETF). An ETF would definitely make it easier for people to invest in Bitcoin, but there still needs to be the demand to want to invest in crypto, which might not automatically be generated with a fund.

Some of the limitations that cryptocurrencies presently face – such as the fact that one's digital fortune can be erased by a computer crash, or that a virtual vault may be ransacked by a hacker – may be overcome in time through technological advances. What will be harder to surmount is the basic paradox that bedevils cryptocurrencies – the more popular they become, the more regulation and government scrutiny they are likely to attract, which erodes the fundamental premise for their existence.

While the number of merchants who accept cryptocurrencies has steadily increased, they are still very much in the minority. For cryptocurrencies to become more widely used, they have to first gain widespread acceptance among consumers. However, their relative complexity compared to conventional currencies will likely deter most people, except for the technologically adept.

A cryptocurrency that aspires to become part of the mainstream financial system may have to satisfy widely divergent criteria. It would need to be mathematically complex (to avoid fraud and hacker attacks) but easy for consumers to understand; decentralized but with adequate consumer safeguards and protection; and preserve user anonymity without being a conduit for tax evasion, money laundering and other nefarious activities. Since these are formidable criteria to satisfy, is it possible that the most popular cryptocurrency in a few years' time could have attributes that

fall in between heavily-regulated fiat currencies and today's cryptocurrencies? While that possibility looks remote, there is little doubt that as the leading cryptocurrency at present, Bitcoin's success (or lack thereof) in dealing with the challenges it faces may determine the fortunes of other cryptocurrencies in the years ahead.

FOR MORE INFORMATION: Search online for the following;

1. 2018 crypto crash
2. Crypto-anarchism
3. Cryptocurrency bubble
4. Cryptocurrency exchange
5. List of cryptocurrencies
6. Chayka, Kyle (2 July 2013). "What Comes After Bitcoin?". Pacific Standard. Retrieved 18 January 2014.
7. Guadamuz, Andres; Marsden, Chris (2015). "Blockchains and Bitcoin: Regulatory responses to cryptocurrencies"(PDF). First Monday. 20 (12). doi:10.5210/fm.v20i12.6198

Compiled by: Afolabi Esther Temitope
July, 2024

THE MAJOR KEYNOTES GOTTEN FROM THE FINANCIAL ACCOUNTING TEXTBOOK
BY AYODELE ASAOLU;

1. Debenture Holders lends money to a business/borrows a company some amount of money while Ordinary Share Holders buy shares in a business and have a fixed percentage on the returns of the business.
2. A Ledger is a book containing a number of Accounts, which are (1)The Nominal Account/Expense Account for items with short-term benefits e.g Wages Acct, Rent Acct e.t.c (2)The Real Account for the physical resources of a company which are either fixed or current assets and (3)The Personal Account for the transactions of all persons with company. While a Trial Balance is a List of All the Balances of other Accounts.
3. Book keeping is the recording of the financial transactions of an organisation in proper and separate books of accounts.
4. Double Entry is when a single transaction involves two entries e.g a wage paid as cash will be recorded both in the Wages Account and in the Cash Account.
5. The loss in an Enterprise is termed Current Expenses while the profit is Current Income.
6. Creditors are those that give goods to an Enterprise on credit, a group of Creditors are called Sundry Creditors and a group of debtors are called Sundry Debtors.
7. Error of omission is when an item is completely omitted from an entry, Compensating Error is when a wrong figure is entered on both sides of a Double Entry Account (NB: The balances will still be equal) while Error of Principle is when a wrong Account is debited or credited (NB: The balance will still be the same).
8. An Invoice is a document made by a seller to be given to a buyer, it contains the details of transaction/purchase.
9. Return of Goods occurs when purchased goods are returned to a supplier (Purchase Return) and if a buyer returns goods/part of the goods, it is Sales Return, Credit notes are given to acknowledge the receipt of goods returned, they are written documents different from an invoice and often printed in yellow or pink colour. Now, Goods can be returned if: (1)they are inferior in standard compared to the specimen on which the order was based, (2)they are damaged on transit before getting into the customer's hand and lastly (3)if the invoice has an error leading to overcharge.
10. The Journal is a subsidiary book which records details of any financial transactions that cannot be recorded in any other subsidiary book. These details help to avoid error in the Ledger Accounts. The Journal is also used to correct the error in a Trial Balance which does not affect the Total Balance of Credit and Debit. If however there is an error in the Trial Balance and it affects the Total Balance of Credit and Debit, the error is corrected by the use of Suspense Accounts.

11. Bad Debts are debts that there is no hope of the debtor paying back, it is advisable to write-off such debts. However a Bad Debt written-off can be paid by the debtor, such will be recorded in a new account as Bad Debt Recovered. But when a debt is uncertain to be bad, it is called Doubtful Debt i.e there's a guarantee the debt will be paid.
12. Depreciation is the allowance made on Annual basis for the normal wear and tear of Assets of an Enterprise.
13. The Cash Account records all cash receipts and all cash payments done in an Enterprise, the bank account is similar to this as it records all cash receipts and payments But made by cheque. Combining these two accounts into one makes up the Cash Book. The Petty Cash Book records expenses that are very small but numerous and are not recorded into the Cash Book, the practice of this entry is called The Petty Cash System.
14. In Cash deposits, the bank debits a customer in the bank account column of Cash Book and credit them in it's own Books while Debit Transfer is making payments by bank transfer. A Deposit Account is more like a Savings Account but withdrawal of cash from this account is with the issuance of 7 Days Notice and the interest gained cannot be known until the statement of account is gotten.
15. Overdraft is allowing a customer to withdraw more than his/her Account Balance with charged interest on the Overdrafted amount.
16. A Standing Order is an instruction given to the bank to pay a customer's Creditor per time e.g for Electricity, Water bills e.t.c
17. Consumable Stores are payments in respect of consumable materials e.g Postage, Stationery e.t.c
18. Stock Purchase is purchase meant for resale within a current accounting period. When a customer pays immediately for goods purchased, it is a Cash Transaction whereas if the customer is allowed to pay for goods purchased at a later time, it is a Credit Transaction and the transaction is recorded in the Debtor's Account or Accounts Receivable. It will appear as debit and when the buyer pays up, it will be credited.
19. Control Accounts are mere Summations of entries already made on the basis of the Double Entry Principle, it is used to control Ledger Accounts. One of the importance of Control Accounts is it monitors data such as ratios of Creditors to Debtors and also it monitors the efficiency of account clerk's book-keeping and it minimise Fraud.
20. Final Accounts consist of the Trading Account, Profit and Loss Accounts and the Balance Sheet. The Trading Account consists of the buying and selling in a business, while The Profit and Loss Gives a Net Profit or Loss of an Enterprise because it records other expenses not recorded in the Trading Account. The Balance Sheet is a summarized list of an Enterprise's Assets and Liabilities. It is alternatively the State of Affairs of an Enterprise or the Financial Status.

21. Profitability measures whether or not a business is doing well in terms of returns on operations while the ability of a business to meet its day-to-day needs for cash and its liabilities/debts is known as Solvency.
22. Over/Under-Trading is a measure of whether a business is carrying more or less volume of trade than it is financially capable of.
23. The difference between Current Assets and Current Liabilities is known as Working Capital while Quick Ratio deals with Assets that can quickly be turned into cash if Creditors press for payment.
24. Debtors or Creditors Ratio tests whether a business relies heavily on Creditors for the running of the Enterprise.
25. Stock Taking is the records of a Business' Assets that can be turned into Cash, there are (1) Annual Stock taking, (2) Perpetual Stock taking and (3) Periodical Stock taking. Stock Valuation is the monetary aspect of Stock Taking which is only a record of number of Assets.
26. Reserves are part of a year's Net Profit which is not to be shared amongst Shareholders but put back into the Business while Provisions are charged against The Profit and Loss Account for the specific purpose of meeting known specific liabilities even when the exact amount of the liabilities are unknown. Capital Reserve is the funds in a business which might not be distributed ordinarily to Shareholders, it could also mean the opposite of Goodwill.
27. There are some Errors in Accounting, they are; (1) Errors of Omission which occurs when an item is completely left out from the Ledger Accounts, (2) Compensating Errors which are errors of the same amount made on both the debit and credit sides of an Account, (3) Errors of Commission which is when a customer is mistaken for another e.g crediting Alua's Account instead of Alao's, and (4) Original Errors which are errors occurring due to the record of original entries into a wrong book e.g Machinery bought recorded in the Purchases Account instead of the Machinery Accounts.
28. The Manufacturing Account collects costs of production i.e those costs incurred in the process of conversion of raw materials into finished products. Prime costs are costs that are directly traceable to the goods being produced, other costs incurred during the process of production are known as Overhead/Period Costs. The Formula for Production Costs = Costs of direct materials + Direct labour cost + Direct expenses costs (purchases made directly for each of the departments in an organization/business enterprise).
29. Joint Indirect Costs are costs incurred jointly by all the departments concerned in an organization e.g Electricity, rent, audit fees, advertisements e.t.c
30. Partnership can be regarded as the association of two or more people for the pursuit of lawful business (or professional practice) for the purpose of profit making. The Partnership Accounts features the partner's Capital and Current Accounts. New partners

can be accepted and current partnership can be dissolved based on agreement or due to death.

31. Goodwill is the value of a business in excess of its asset value, Goodwill is created when the purchase consideration is higher than the Net Worth of the business e.g a buyer willing to pay #100 for a biscuit pack worth #70, the Goodwill is #30.
32. Trade Mark is the name under which a commodity is being advertised to distinguish from other manufacturers. Patents are exclusive rights of a producer to use certain formulae or produce a kind of product with a brand name.
33. Trade Investments are investments in other trades/buying majority shares in other trades or companies. Listed Investments are investments in companies whose shares are listed on the Stock Exchange.
34. Hire-Purchase is a system of installment payments for goods put on hire.
35. Cash Price is the price for which an asset would be sold.
36. Consignment Account is a special Account prepared in respect of goods service to an agent who is to sell goods on behalf of the principal. Consignment Outwards are the goods sent out to agents. Agents Commission is the remuneration payable to agent on sale of goods on consignment while Del Credere is a special type of commission payable to an agent who accepts responsibility for all debts in respect of sale of goods in consignment.
37. Contract Account adopts a system of matching contract expenses against prices and Periodical monitoring and reviewing of the work done so far. Retention Money is the percentage of the contract price for a period of six months after completion of contract. This is to ensure that any likely errors or faults in the execution of contracts are rectified.
38. Public Service Accounting is basically the system of Accounting used by the Government or the Civil Service to keep Records of Government revenue and expenditure.
39. Cash Distribution Register shows the opening balances, receipts, payments and closing balances of ALL Treasury in a State.
40. Data Processing is the process of organising information by the use of computers. Data can be processed through; (a) Manual Method: using man's physical and mental efforts alone, (b) Mechanical Method: this involves the use of machines, it is complemented by human effort which facilitates its effectiveness and (c) Computer Method: by the use of electronic devices. This happens when any kind of computer is engaged to facilitate Data Processing.
41. Accounting Conventions are fundamental ideas, concepts or assumptions that are usually accepted by all Accountants in the recording and preparation of Financial Statements. Accounting Cycle is a process by which invested Capital circulates throughout the Enterprise of a business.
42. Accrual indicates benefit(s) consumed during a period for which no payment has yet been made.

- 43. $\text{Average stock} = \frac{\text{Opening Stock} + \text{Closing Stock}}{2}$
- 44. Cash Flow is the amount by which the internal cash resources of a business have increased.
- 45. A Crossed cheque means a cheque that can only be cashed out by depositing it in a bank account. It may contain the Payee's bank, branch or Account Number. A Crossed cheque has a double parallel line across it diagonally.
- 46. Current Ratio is the ratio of current assets to current liabilities and Current Assets are short-term nature in a business e.g Cash to Raw Materials to Finished goods to Debtors/to Cash (they change from time to time in the course of the business). Intangible Assets are assets that do not possess any physical existence but represent the value of a right e.g Goodwill, Patents, Trademarks e.t.c
- 47. Obsolescence of an Asset is the drop in the value of an asset due to invention of better and more economic methods.
- 48. Real Accounts are the accounts kept for the assets of an organization.

Compiled and submitted by: Afolabi Esther Temitope

29th of April, 2023

GUIDELINES TO A SUCCESSFUL MARITAL DESTINY

Jeremiah 29:11&12 is God Himself telling man (both male and female) that He has a good plan for the future and also HOPE. This is coming from the omniscient (All-knowing) so it is TRUE/THE TRUTH.

The human mind is uncertain of the happenings of the future and this causes fear in the heart of men especially when it comes to the issue of having/choosing a life partner. However, God has a good plan for us and that is our confidence, provided we follow the principles for it.

Now, in Genesis 2:18, GOD SAW that it was not good for the man to be alone as helpless as he was. Notice, it was not the man's doing nor his will but in verses 20b-25, it was explained how that God's suggestion of a helper pleased the man (male). Adam SAW (sight/perception) the female and knew (discernment) that she was made out of him (part of him and his totality).

If this chapter 2 is read from its beginning, Adam already had an assignment which he was carrying out in the garden of Eden and God saw that he needed to be helped. Adam was not idle, he knew exactly what he is to do in the garden and he followed every instructions given to him until the FALL OF MAN.

Genesis 24 is another example of a marriage procedure, Abraham must have known that he has to protect the covenant if God upon his generation and Isaac marrying a strange woman with a strange/different covenant will not be the best so he had to make his servant search for a relative with whom to share this covenant of the Lord.....this explains that as a believer, we can only marry our relatives which are Believers. Marrying an unbeliever is not an option to be considered in the kingdom of God, 2cor 6:14-16.

Marriage/choosing a life partner for a believer in Christ is basically on Instructions and less of Personal Will, take a look at the life of prophet Hosea that was instructed to marry an adulterous woman, no man would want to marry a harlot not to talk of a prophet that is a symbol of God's holiness amongst people. Hosea did accordingly to the word of God and God's purpose was fulfilled.

In choosing a partner, this should be established: God decides. There is a lie from the pit of hell that God will not choose what we would like but who knows us better than our creator and who knows better than him who will be suitable for us? The western culture of dating as made things worse, many marriages are built purely on self will and emotions at times list and the result; DIVORCE, God hates divorce so why would he chose the right person for us?

Some things to consider when choosing a life partner;

7. Ask God: no one asks and does not receive. Matthew 7:7

8. Be patient: this will help you avoid falling into error as you have committed everything to God's hands so rest your fear.
9. Be friends: Even after discerning who to marry, try as much as possible to be friends with the person, this will give room for mutual understanding and corrections can be made effectively.
10. Seek parental consent: Parents are experienced and God commanded us to obey them. In a case where God has said go on but the parents are unwilling, commit their hearts to God and be wise in waiting.
11. Train your spouse: whether male or the female gender, don't expect your spouse to change overnight after wedding, start training yourselves during courtship.
12. Build character e.g Patience, self control e.t.c
13. Essentially, discover your Vision as a male before asking the female to join your journey.
14. As a female, prepare yourself to fit into the vision of your future spouse, don't just sit and waste away.

SOME THINGS TO AVOID;

8. Rush: there is no need for you to rushing because God is always on time, never late.
9. Rebellion against God & parents: no chastising is sweet now until the fruits start to ripen. Some of your will may be ignored if they aren't borne out of genuinity and it may seem as if God does not understand you/he is punishing you, just hold on and obey.
10. Trial and error method: Dating as it is called is a trial and error method of approach to marriage and it is not Biblical nor Godly. This method has thrown many hearts into life time sadness and the only way out is no to be involved. There is no crime in being friends with an opposite gender but know you boundaries and save yourself the heartbreak.
11. Emotional interference: God created this as a blessing so harness its power for good not otherwise. Our emotions should not over take our head in matters like this because whatever our choice is will affect many generations, be wise.
12. Sex before marriage: sex is a way/act of initiating a covenant with your spouse that you are one and it brings blessings when done aright (in marriage) but if done without God's consent, it is dangerous and it brings curse plus other effects like emotional distress, uncertainty, insecurity and the likes.

In all your getting, get wisdom. It's is the principal thing. I pray that God will help us into his will for our marital lives.

