IJRESM
International Journal of Research in Engineering, Science and Management
Volume 7, Issue 2, February 2024
https://www.ijresm.com | ISSN (Online): 2581-5792

Advancing the Account Aggregator System in India Leveraging Blockchain Technology and Homomorphic Encryption

Mahir Patel*
Student, Department of Science, Essar International School, Surat, India

***Abstract*: The increasing reliance on data sharing for financial services exposes the limitations of traditional data collection methods, necessitating a more efficient and secure framework. The 2024 budget allocation for technology and financial inclusion initiatives signifies the government's commitment to innovation and accessibility in the financial sector, providing momentum for the growth of the Account Aggregator (AA) system. However, the AA system faces critical challenges such as data security vulnerabilities and consent management complexities, hindering its ability to effectively serve India's economic needs. To address these challenges, this paper advocates for integrating blockchain technology and homomorphic encryption within the AA framework. Firstly, it explores the working, history, and applications of the framework released in 2021, followed by an analysis of key predicaments and overall effects. The technical aspects of blockchain technology and homomorphic encryption are then examined to understand their potential contributions to the AA system. Blockchain's decentralized ledger offers tamper-proof data storage and transparent transaction records, enhancing security and auditability. Homomorphic encryption enables secure computation on encrypted data, ensuring privacy and confidentiality throughout data transactions. By leveraging these technologies, the AA system can overcome its existing limitations and better meet the economic needs of India's populace. This paper provides a comprehensive solution with strong potential to enhance the effectiveness and security of the AA system.**

***Keywords*: account aggregator system, blockchain technology, homomorphic encryption.**

1. Introduction

India's remarkable growth in the financial sector, marked by transformative initiatives such as the Unified Payments Interface and the Account Aggregator system, underscores the nation's commitment to nurturing financial inclusion and digital innovation. These initiatives have revolutionized the way financial transactions are conducted, empowering millions of Indians with convenient and secure digital payment solutions. However, despite the strides made, the AA system faces critical challenges that impede its full potential. A comprehensive analysis by the Economic and Political Weekly sheds light on these issues, highlighting concerns such as data security vulnerabilities, consent management complexities, and the need for greater user awareness. Many Indians, particularly those from rural and marginalized communities, may not fully grasp the implications of sharing their financial data through the AA system which raises ethical concerns and underscores the importance of transparent communication and user-friendly interfaces. Furthermore, data privacy ethics emerge as a dominant concern. With the exponential growth of digital transactions, ensuring the confidentiality and security of personal financial information is essential to maintaining trust and confidence in the digital economy. The integration of blockchain technology and homomorphic encryption within the AA framework helps overcoming the limitations and pave the way for a more inclusive and secure financial ecosystem. The decentralized ledger of blockchain offers a tamper-proof data storage addressing the accountability and security issues, unlike the current centralized data storage. While, homomorphic encryption enables secure computation directly on encrypted data that preserves both privacy and allows a meaningful analysis. Through a comprehensive examination of these solutions and their implications for India's digital economy, this paper aims to provide a roadmap for advancing financial data sharing and fostering trust and transparency in the digital age.

2. Account Aggregator System

A. Definition of the AA system

In this digital economy, data bias disproportionately impacts the consumers in the financial sector harshly, especially the ones with restricted choices due to factors like geographical location, social standing or economic status. To eliminate such predicaments, India introduced the Account Aggregator system in 2016.

"An Account Aggregator is a type of Non-Banking Financial Company regulated by the Reserve bank of India that enables individuals to securely and digitally access and share their financial information from one financial institution to another within the AA network. The AA ecosystem consists of Financial Information providers (FIPs) and Financial Information users (FIUs) that hold and seek the individual's data." - (Press information bureau of Delhi: Ministry of Finance, 2021)

In simple terms, the AA system acts like a web crawler for

*Corresponding author: mahira.patel@icloud.com

an individual's financial information. Akin to how a web crawler accesses data from different websites without needing the client to visit each website separately, the AA system lets an individual access his/her financial data from various banks, insurance companies and other financial institutions in one place.

B. *The Background of the AA-system*

The Account Aggregator (AA) framework was first conceptualized in India in 2016 and was officially notified via the RBI Master Directive in September 2016. The framework was created through an inter-regulatory decision by RBI and other regulators, including Securities and Insurance Regulatory and Development Authority, and Pension Fund Regulatory and Development Authority (PFRDA), through an initiative of the Financial Stability and Development Council. The license for AAs is issued by the RBI, and the financial sector has many AAs. The AA framework was introduced in India in September 2021 and is part of India Stack, a collection of open-source APIs by the Government of India.

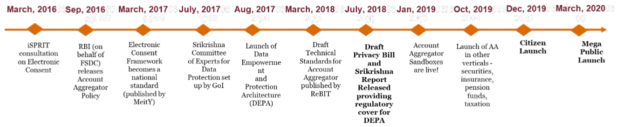
March, 2016
Sep, 2016
March, 2017
July, 2017
Aug, 2017
March, 2018
July, 2018
Jan, 2019
Oct, 2019
Dec, 2019
March, 2020
iSPRIT consultation on Electronic Consent
RBI (on behalf of FSDC) releases Account Aggregator Policy
Electronic Consent Framework becomes a national standard (published by MeitY)
Srikrishna Committee of Experts for Data Protection set up by GoI
Launch of Data Empowerme nt and Protection Architecture (DEPA)
Draft Technical Standards for Account Aggregator published by ReBIT
Draft Privacy Bill and Srikrishna Report Released providing regulatory cover for DEPA
Account Aggregator Sandboxes are live!
Launch of AA in other verticals - securities, insurance, pension funds, taxation
Citizen Launch
Mega Public Launch

Fig. 1.

The AA framework has been growing in market adoption across banking, securities, insurance, and pension sectors. On September 2, 2021, eight of India's major banks, including State Bank of India, ICICI Bank, Axis Bank, IDFC First Bank, Kotak Mahindra Bank, HDFC Bank, IndusInd Bank, and Federal Bank, joined the AA network that enables customers to easily access and share their financial data. The AA framework has been adopted by several banks and financial institutions in India, and it has revolutionized the lending ecosystem by enabling individuals to access credit and other financial services more easily, leading to increased economic activity and cost savings for lending institutions. The AA framework is designed to empower individuals with control over their financial data and enable seamless and secure access to financial services. It prioritizes data privacy and security, and the account aggregators are required to comply with the RBI's directives around data security and the upcoming data protection legislation. The AA framework is expected to expand beyond the financial sector to allow access to healthcare and telecom data, further enhancing its impact on the economy and individuals' financial lives. The AA framework has gained prominence due to its potential to drive digital lending, open banking, and financial inclusion in India.

C. *The mannerism and working of the AA system*

The key characteristics that led to the accent of this system are as follows:

1) *Key players in the account aggregator system*

Financial Information Providers or FIPs: Institutions that hold user data, such as banks, mutual fund houses, insurance providers, income tax/GST platforms, and other financial institutions are referred to as FIPs. They serve as the custodians of the user's financial data and are responsible for providing this information to AAs upon the user's consent. The data shared by FIPs may include information related to bank accounts, mutual fund investments, insurance policies, tax filings, and other financial records.

Examples: State Bank of India, ICICI Bank, Axis Bank, IDFC First Bank, mutual-fund houses, insurance providers, income tax/GST platforms, etc.

Financial Information Users or FIUs: Entities that use the financial information provided by FIPs through the AA system are referred to as FIUs. They can be any entity registered with and regulated by a financial sector regulator, such as banks, mutual fund houses, insurance providers, income tax/GST platforms, stockbrokers, registered investment advisers, and portfolio managers. FIUs use the financial data to provide services to customers, such as credit, insurance, wealth management, and loans, based on the financial data received from the FIPs.

Tech Service Providers: Tech service providers in the AA system facilitate the secure and efficient sharing of financial data between FIPs and FIUs. They are certified by the Reserve Bank of India as Account Aggregators and are responsible for:

1. Ensuring the authenticity of the documents since they source them directly from the financial entities.
2. Facilitating the flow of data through Application Programming Interfaces.
3. Complying with the RBI's directives around data security and the upcoming data protection legislation. Examples: Finvu, OneMoney, CAMS Finserv, NESL, PhonePe

Certifiers: Certifiers in the AA system are responsible for ensuring that the tech service providers adhere to the RBI's guidelines and regulations.

2) *Working*

Suppose you have multiple bank accounts, credit cards, and investment accounts with different financial institutions. It can be challenging to keep track of all these accounts separately and manage your finances effectively. This is where the AA system comes in. When you sign up for an AA service, you give them permission to collect your financial information from different banks, insurers, and investment firms that you have accounts with. This information includes your account balances, transactions, and other relevant details. Once the AA collects this data, they organize and present it to you in a user-friendly format. You can then view your overall financial picture, track your spending, monitor investments, and even apply for loans or other financial services directly from the AA platform.

For example, let's say you have a bank account with Bank A, a credit card with Bank B, and an investment account with Brokerage C. You sign up for an AA service and provide your consent to share your financial data with the AA. The AA collects your financial data from Bank A, Bank B, and Brokerage C and presents it to you in a single dashboard. You can view your account balances, transactions, and investment performance in one place, making it easier to manage your finances. You can also use the AA platform to apply for loans or credit cards, as the AA already has your financial data and can pre-approve you for certain financial products.

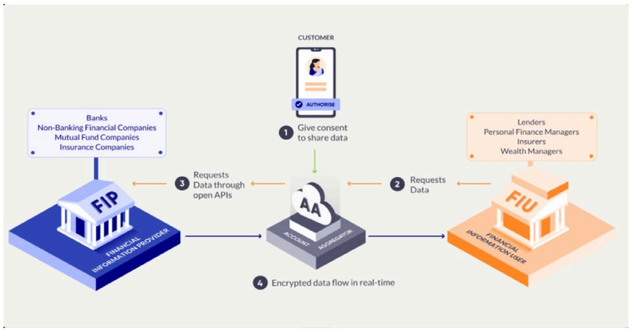
CUSTOMER
AUTHORISE
1 Give consent to share data
Banks
Non-Banking Financial Companies
Mutual Fund Companies
Insurance Companies
Lenders
Personal Finance Managers
Insurers
Wealth Managers
3 Requests Data through open APIs
2 Requests Data
FIP
FINANCIAL INFORMATION PROVIDER
AA
ACCOUNT AGGREGATOR
FIU
FINANCIAL INFORMATION USER
4 Encrypted data flow in real-time

Fig. 2. Explanation diagram of AA system *(Sahamati)

3) *Impending challenges and the way forward*

While the AA framework has the potential to drive digital lending and open banking in India, several challenges must be addressed for it to realize its full potential:

i. *Data privacy and security*: Ensuring the privacy and security of consumer data is crucial to the success of the AA framework. Financial institutions and account aggregators must implement robust security measures, such as data encryption and multi-factor authentication, to safeguard consumer data and build trust in the system.

ii. *Financial literacy*: To take advantage of the AA framework, consumers must be educated on the benefits of sharing their financial data and how to do so safely. Financial institutions, account aggregators and the government should collaborate to promote financial literacy and raise customers' awareness and understanding of the AA framework.

iii. *Interoperability*: The AA framework must be built on a foundation of interoperability to facilitate seamless data sharing among financial institutions. Standardization of data formats and protocols is essential to ensuring the compatibility of systems and smooth data exchange.

Furthermore, to foster the growth of neobanks, a supportive regulatory environment is essential. Regulators should nurture innovation while maintaining appropriate safeguards and consumer-protection measures. Collaboration between regulators, traditional banks and neobanks is vital to striking a balance between promoting competition and ensuring a level playing field.

The AA framework represents a significant step forward in India's journey toward a more inclusive, competitive and customer-centric financial sector.

D. *Current Affairs of the AA System in India*

1) *Expansion and Adoption Across the Financial Ecosystem*

The AA ecosystem has experienced remarkable growth, with over 1.1 billion AA-enabled accounts and 2.05 million users engaging in voluntary financial data sharing. This widespread adoption is not just limited to consumers but extends across major public and private sector banks, further bolstered by the inclusion of SEBI. This expansion signifies a robust foundation for financial data sharing and interoperability, setting a precedent for digital financial services in India.

2) *Empowering MSMEs with Enhanced Credit Access*

The AA framework is instrumental in streamlining the financial inclusion of Micro, Small, and Medium Enterprises (MSMEs) by mitigating traditional hindrances such as procedural delays and excessive paperwork. Given the pivotal role of MSMEs in driving economic growth and employment, improving their access to credit through the AA framework is a critical step towards leveraging their potential for India's economic development.

3) *Synergy with the National Financial Information Registry (NFIR)*

The integration of the NFIR with the AA network is a strategic move to democratize access to credit. By facilitating easier creditworthiness assessments, the NFIR aims to enhance the flow of credit, especially to underserved segments of society. This synergy is expected to unlock new avenues for cash flow-based lending and contribute significantly to financial inclusion.

4) *Revolutionizing Digital Lending*

The AA framework is at the forefront of a digital lending revolution, making financial services more accessible and efficient. By enabling detailed and secure financial data sharing, it opens up credit access to broader segments, including those without traditional credit histories. The framework's capacity to streamline the lending process and provide comprehensive data for credit assessment positions it as a cornerstone for innovative lending solutions.

5) *Advancing Open Banking*

The AA framework is catalyzing the open banking movement in India by fostering a more competitive and innovative financial marketplace. Through data democratization, it empowers consumers to control their financial data, thus encouraging financial institutions to develop more personalized and consumer-centric products and services. This environment of enhanced competition and innovation is pivotal for the growth of a dynamic financial sector that is responsive to consumer needs and preferences.

6) *Potential to Mirror UPI's Success*

Drawing parallels with the transformative impact of UPI on payments, the AA framework, supported by regulatory innovations such as Video KYC, is poised to redefine digital lending and financial inclusion. The Finance Minister's advocacy for the AA framework underscores its potential to significantly enhance access to credit, thereby catalyzing economic growth and inclusion.

7) *The Critical Role of Account Aggregators*

Account Aggregators, licensed as non-lending NBFCs by the RBI, are the linchpins in the AA ecosystem, facilitating secure and efficient data sharing between borrowers and lenders. This role not only streamlines the KYC process but also enriches the credit evaluation process, thereby enhancing the efficiency, accuracy, and reliability of financial services.

3. Problems & Major Bugs

Worldwide, Similar schemes have been implemented to enable the sharing of bank account information through a new status of institutions. The account info service provider system (AISP) instituted by the officials in the United Kingdom is one example. However, these AISPs only provide information in a series of steps and none matches to the level envisaged by NBFC-AA. Thereby, making it imperative for us to carefully examine the tenets of its programme.

Conspicuously, this project has caught the scrutiny of entrepreneurs, policymakers and the media in India. In today's digital economy, with all certainty, the predicaments that AA aims to settle are legitimate. With the RBI announcement of master directions and the Reserve Bank Information Technology Private Limited's technical architecture for the AA system, this could very well become the de facto method to use or purchase a range of financial services including mutual funds, insurance, credit products, etc. (RBI 2016; ReBIT 2019).

Regarding the concern of digital delivery of financial services, the AA has the potential to act both as the midwife and the executioner at the same time. It has never been easier to access data of a large number of individuals at such low costs, but these individuals have never been subject to a more comprehensive profiling programme either, which can reconcile multiple data sets from across the board.

Yet, there is a need to ask if the architectural foundations which the AA operate on level up to the requirements of an ecosystem that is likely to touch the lives of 140.76 crores citizens of India Can we as the consumers of this system, be content with the balances and checks that have been put in place to monitor the working of the AA system?

A. Subduing the User Agency

When one buys a financial product, the seller requires the buyer to provide certain specific information that allows the seller to price the risk of the transaction appropriately. Traditionally, before the surfacing of Aadhar's e-KYC, this was provided by the buyers or consumers directly to the seller or provider or affiliate appointed by the provider. The verity of the documents provided was also attested to by the consumers themselves. For example, providing a fake bank statement to avail a loan constituted a fraud. However, such a transaction in past did not affirm the presence of a third party to verify or mediate it. In other words this traditional method of transaction did not upend the agency of the user.

A principal feature of the AA architecture is that the users delegate the sharing of their financial information to a third party that is the AA. The third party then takes the role of first by securing the information from a provider and then temporarily stores the information before providing it to the entity requesting it. The user is provided with bare details concerning consent mechanism, which is likely to be miscomprehended inadvertently.

The election of such an architecture is reflective of the fundamental thought process that puts the AA ecosystem's needs above that of the consumers. The gospel that the user has no means to offer verified data directly to the third-party financial parties in lieu of a service, without the involvement of a third party, is reminiscent of the architecture that Aadhar provided until the offline KYC process was introduced in 2018 after a long legal battle and public anger. (Khera 2019)

Using the AA ecosystem demands the individuals to only act through a mediator. This invites multiple risks of errors, both false positive and false negative kind at different touchpoints. Technical glitches at AA's end could cause imprecise responses, which could end up clogging the access of deserving individuals to financial products. While the technical standards do acknowledge security checks to prevent such things from happening, it is not hard to imagine such accidents as evidenced in the case of Aadhar or UPI set up. (Alam 2018)

Though it could be cognised that individuals would have the preference of using a different system to share their data, it is highly unlikely that the AA system will end up exerting a forceful network lock-in, which could make it much harder for individuals to employ alternatives to share their financial information securely.

B. The Architectonics of the AA System

The architecture of AA system, as introduced, creates a number of trade-offs that could delegitimize the privacy of the consumers and also put the system itself at risk:

1) Issue of data ethics

The AA system can be used as a large-scale mechanism for data mining by FIPs and FIUs. Suppose a food delivery application, like Swiggy, starts offering one an option to purchase on credit. In order to enable such a programme, for example, one is required to share his/her income and account statement to verify their worthiness for credit. Giving such information through an AA would mean that Swiggy can use the previous history of spending and offer food at a differential price, or use that information for targeted advertising. For example, knowing that one often eats pizza, the company can target him/her for advertisements from pizzerias even if one hasn't ordered pizza from Swiggy before.

While technical specifications and PDP bill do have provisions on purpose-limitation and the restrictions on data storage, there is nothing that can prevent a FIU from overreaching and taking a wider variety of permissions.

UK's financial conduct authority, tasked with regulating open finance for the UK market in its "Call for input on Open Finances", specifically highlights the issue of data ethics arising out of the interconnected systems. The use of Artificial Intelligence and Machine learning and the risk of perpetuating existing biases and prejudices present additional potential risks emerging out of open finances (FCA 2019).

Further, nothing in the AA framework or the PDP bill explicitly stops FIUs of any kind from combining their existing databases with financial information to profile their consumers. This makes AA system conducive for data mining, thereby arising ethical issues. If truth be told, the specifications, presently, do not enforce any standards on how an FIU, after obtaining the financial information from an AA, would be required to store and manage data. (Raghavan and Singh 2018)

2) Probability of abuse and data mining

The guidelines set forth by RBI;s master directions doesn't allow the AA to permanently store the data that has been fetched and stored by it, in receipt of the consumer's consent. It is required to prescribe a time frame within which the FIU must take the information from the temporary data storage of the aggregator. The information may be stored with the AA for a maximum of 72 hours. However, the technology guidelines fall short of mentioning a method to enforce the impermanence of the storage. (NeSL 2021).

C. Pandemonium of Consent Collection

"The master directions of RBI mandate FIPs to share financial information of a consumer with an AA when the latter presents a valid consent. Added, it is compulsory that FIPs verify the consent before the requested information is shared with the AA" (ReBIT 2019).

However, the technical specifications introduced by ReBIT, dispense no method as to how the consent could be expressed, in terms of the actual interface design to the consumers. This is specifically a risk since it has been brought to attention numerous times that individuals consenting to the terms online often have a poor understanding of what they are consenting to. If we are to solely rely on the consent collection specifications issued under Electronic Consent Framework, v1.1, published by the Ministry of Electronics and Information Technology, it could turn out to be fret. The specifications suggest that a consent collector can possibly obtain the consent by simply "having the user click a button or by signing a paper form" (MeitY nd).

Furthermore, a number of supplementary problems regarding to consent collection have been identified by researchers in this process:

1) Consent friction and debility

It is believed that mere disclosure policies would not be enough for individuals to make a meaningful choice. Almost in all cases, consent forms or pop-ups are presumably going to be ignored by the consumers because it adds a blanket of friction to the otherwise seamless browsing experience. The internet as an approach is familiar to inadvertently favour interfaces that reduce friction. This blanket of friction conjoined with consent debility could lead to a devaluation of consent, where the consumers just affirm to whatever terms and conditions of service, and furnish their consent without bothering to read the details of what they are consenting to (Matthan 2017).

2) Misinterpretation of terms and policies

Most consumers find the consent mechanism futile when it comes to actually guarding their privacy. In fact, often, not only do individuals fall short in understanding the fine print of privacy policies, but also often misunderstand the policies as guarantees of data protection, instead of liability disclaimers for firms, a phenomenon known to be called "privacy paradox" (Blank et al 2014).

3) Forging consent as a governing factor of service

Blatant reliance on a consent-based architecture implies that institutions are no doubt adopting a "take it or leave it" approach, wherein the consumer is paraded with the only possible course of action of not using the service at all unless they consent to their data processing jurisdiction. This heterogenous manipulation of consent mechanism puts forward the individual with a false choice and the illusion of control. (Raghavan and Singh 2020)

4) Absence of feature phone support

Another concern raised by a recent research elaborates with the consent architecture within India's account aggregator system, particularly for feature phone users who may lack reliable internet and electricity. The cornerstone of the AA system is informed consent, a principle that is essential for legally collecting, using, and disclosing personal data.

The PDP bill establishes guidelines for data collection notices. However, the practicality of obtaining genuine consent given the current technology and business models is questionable. Despite these complexities, it is crucial to uphold the principles of consent as envisaged by the bill. As internet usage grows, the demographic of users is skewing towards young women and rural populations, groups often marginalized and at higher risk of online threats. It is critical to bolster consent procedures and notification processes to protect these users.

A potential solution is the introduction of a 'layered notice mechanism' at the point of consent collection to aid user understanding. This approach would provide a balance between usability and the seriousness of the transaction. It's also important for notices and consent forms to be accessible, suggesting that account aggregators should use visual aids like standardized icons to communicate more effectively with users who may not be proficient in English.

D. Right to Information on Data Breach

The PDP bill requires that data fiduciaries should inform the protection authorities about the breach of any personal data processed by them, and whether if such breach is supposed to cause the data principal i.e. the consumer any harm or not.

However, the bill leaves it completely to the protection authority to decipher whether the information related to the breach should be reported to the principal or not. This is a plain detour from the perception that the notification of data breach should be considered as a "right" of the consumers, an ideology that has been ascendingly gaining ground since the EU commission introduced it in 2015 (Whittaker nd). This gives data subjects the right to know when their data has been mal-practiced or hacked, through notification by data controller to the consumer or the national supervisory authority. This allows consumers to take immediate action to limit the mutilation, and also to prevent data controllers to hide their errors. This is an important concern since financial institutions, including bank and payment systems, are known to be hacked on several occasions, and the consumers' personal data is compromised or put under the risk of compromise.

The AA are designated to carry very sensitive data about their consumers, and are probable to be targeted by external hackers.

E. Structural Predicaments

In addition to the above list, we foresee some necessary challenges arising due to the structural set up of the system. These ensue either directly from the architectural choices or due to the externalities that may largely impact the running of the AA programme.

1) Overuse of consumer data

In developing economies across the globe, when the authorities subsidise the cost of public resources, like water or salt, its supply goes up, but it also decreases the social value, and so people end up consuming more of it, and the demand increases. The social cost of this subsidy shows up in what economists call "deadweight loss", a reflection of increased consumption at lower social value driven by artificial costs (Tabarrok and Cowen 2017).

Although data, unlike water or salt, is not necessarily a limited resource, it would be wise to include a similar mindset when handling the financial information of the consumers. The worry is that the availability of the infrastructure could easily encourage the FIUs to abuse the system in taking as much data about the consumer as possible. Decreasing the costs of accessing consumers' data and its consequent availability in plenitude would decrease its value. While such an approach may help the FIUs or AA, it will come at an extraordinary cost to the individuals and even the society as a whole.

It would be clever for the AA system to structurally incentivise FIUs, which needs fewer data points over the ones that need more. For instance, a lender, utilizing the system, which requests for fewer data points to decide the credit worthiness of an applicant should be encouraged over one that asks for multiple data sets. Relying exclusively on consumers to make this decision for themselves may not really work, especially since they would not be able to appropriately price their own privacy.

2) Interoperability concerns

There could be many explanations as to why FIPs might not share or make it difficult to share consumer data with other firms. The primary reason for this could very well be commercial. Sharing of data can risk the disruption of business models or market share of a data-rich incumbent. The firms may wish to avoid the setting up and maintenance costs of sharing the data or may be dissuaded by the ROI from sharing the financial information of the consumers.

Interoperability problems among financial institutions were noticed during the inaugural days of UPI when a major bank had blocked transactions from one of the UPI applications (Variyar 2017). Such a situation could very well play out again with the AA system.

3) Organisational structure of the AA

The master directions of the RBI stipulate a number of requirements for a company that wishes to apply for a license to become an AA. However, the rules do not preclude the companies that are already operating in the consumer finance space from applying for the license. There are two possible risks that we see coming out of this.

The first is that the AA with a parent institute, that offers a service or a product that directly competes with the one offered by an FIU, makes it difficult for the FIU to obtain customer's data. This is the interoperability concern expressed above. The second risk is that the AA, upon scrutinising that the consumer is interested in an external entity's offering that competes directly with its own could proffer or incentivise the customer with targeted messaging to switch from external FIU to the AA licensed institute.

For instance, Jio, a wholly owned telecom subsidiary of Reliance industries. It operates the country's largest network and has a payment banking license, license to issue payment cards and has applied to operate as an AA and gotten approval (Pathak and Borate 2020). Jio could possibly use the AA license with its existing muscle to build a walled chain around its consumers exerting a strong lock-in that could make it very difficult for the consumers to exercise their choices freely.

4. Blockchain Technology

A. Understanding of Blockchain Technology

Blockchain is one of the major tech stories of the past decade. Everyone seems to be talking about it, but underneath the chatter there isn't always a clear understanding of what blockchain is or how it works. Despite its repute for impenetrability, the basic ideology is pretty simple and it has major potential to change industries from the bottom up.

"A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network" (Synopsys)

Blockchain owes its name to the way it stores a transaction data-in blocks linked together to form a chain. As the number of transactions grows, so does the chain of blocks. Blocks record and confirm the time and sequence of transactions, which are then logged into the blockchain, within a discrete network governed by rules agreed to by the network participants. (Tiana Laurence 2017).

B. History of the Technology

The journey of blockchain technology commenced with the foundational work in cryptography, marked by the publication "New Directions in Cryptography" in 1976. This pivotal moment in the history of digital security was followed by another significant paper, "How to Time-Stamp a Digital Document," authored by Stuart Haber and Scott Stornetta in 1991. Their work introduced the groundbreaking concept of timestamping digital data instead of its physical carrier, laying a foundational stone for blockchain's development.

Further advancing the field, David Chaum proposed a digital currency and electronic cash system, envisioning a new era of financial transactions. In 1997, Adam Back's "Hashcash" addressed email spam through proof-of-work, a concept that also inspired Wei Dai's "b-money" proposal for a decentralized, peer-to-peer currency system (Sarmah, 2018).

Initially, blockchain technology aimed to facilitate trustworthy peer-to-peer financial exchanges without the need for intermediaries.

Satoshi Nakamoto's seminal paper, "Bitcoin: A Peer-to-Peer Electronic Cash System," published in 2008, elucidated the use of cryptographic hashes within a block system. This innovation offered a solution to the double-spending issue through a decentralized, peer-to-peer network, establishing a verifiable sequence of transactions. This system not only fostered trust in electronic payments but also ensured their irreversibility, marking a significant leap forward in secure digital transactions (Nakamoto, 2008).

In the wake of this publication, open-source software was launched to operationalize blockchain through the introduction of Bitcoin, the first cryptocurrency, in early 2009. This initiative by Satoshi Nakamoto led to the genesis of the first Bitcoin network and the inaugural series of Bitcoin transactions. The year 2010 witnessed the first recorded purchase with Bitcoin—10,000 bitcoins for a pizza—underscoring the currency's potential. By 2013, the Bitcoin marketplace had burgeoned to exceed $1 billion in value, illustrating the revolutionary impact of blockchain and Bitcoin on the financial landscape.

That same year, Vitalik Buterin published the white paper "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform," introducing Ethereum as the second-generation cryptocurrency. Ethereum extended blockchain's utility beyond simple currency transactions by integrating smart contracts and decentralized applications (dApps). These dApps operate on a decentralized network, leveraging smart contracts for backend operations while allowing for a diverse range of frontend user interfaces. This innovation represented a significant evolution in blockchain technology, enabling a wide array of applications beyond financial transactions and establishing a new paradigm for decentralized digital services (Buterin, 2014).

C. Blockchain Architecture

Blockchain is a sequence of blocks which holds a complete list of transaction records like a conventional public ledger [14].

Figure 3 illustrates an example of a blockchain. With a previous bock has contained in the block header, a block has only one parent block. It is worth noting that the uncle blocks (children of the block's ancestors) hashes would also be stored in Ethereum blockchain [15]. The first block of a chain is called genesis block which has no parent block.

1) Block

A block consists of a block header and a block body as shown in figure 4. Specifically, the block header includes:

i. Block version: Indicator of the set of block validation rules that need to be followed

ii. Merkle tree root hash: Hash value of all transactions in the block

iii. Timestamp: Current time as seconds in universal time since January 1, 1970.

iv. nBits: Target threshold of a valid block hash.

v. Nonce: A 4-byte field, that generally starts with the 0 and ascends for every hash calculation

vi. Parent block hash: A 256-bit hash value that points to the previous block.

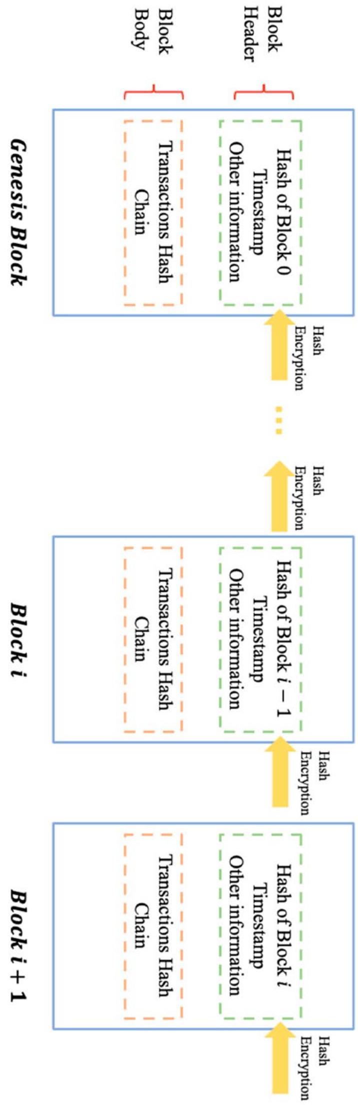

Fig. 3. An example of blockchain which consists of a continuous sequence of blocks (IJERPH 2022)

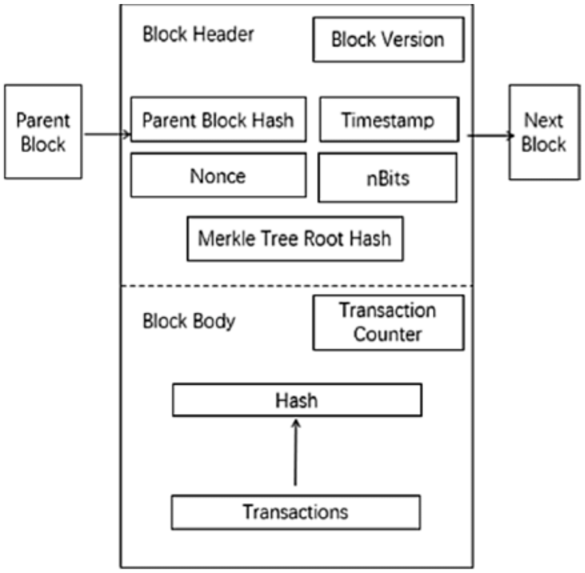

Fig. 4. Block structure (Sonali Chandel 2020)

Table 1
Differentiation between public, private and consortium blockchains

Property	Public	Consortium	Private
Consensus Determination	All miners	Selected set of nodes	One organization
Read Permit	Public	Public or restricted	Restricted
Nature of mutability	Impossible	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralized or not	No	Partial	Yes
Consensus Process	Permissionless	Permissioned	Permissioned

The block body consists of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on its size and the size of each transaction. Blockchain uses an asymmetric cryptography mechanism to authenticate the transactions [13]. Digital signature based on asymmetric cryptography mechanism is utilized in an untrustworthy environment.

2) *Digital Signature*

Each consumer owns a pair of private key and public key. The private key is used to sign the transactions and indeed is kept confidential. The digital signed transactions are broadcasted throughout the whole network. The typical digital signature is involved with two phases: signing phase and verification phase. For example, an user Ross wants to send another user Rachel a message. In the signing phase, Ross encrypts his data with his private key and sends Rachel the encrypted result and original data. In the verification phase, Rachel verifies the value with Ross's public key. In that way Rachel could easily see if the data has been tampered or not. The typical digital signature algorithm used in blockchains is the elliptic curve digital signature algorithm (ECDSA) [16].

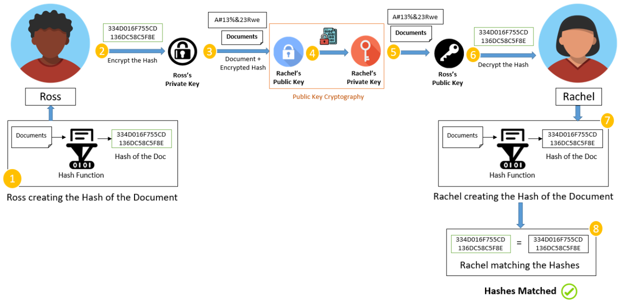
334D016F755CD 136DC58C5F8E
2
Encrypt the Hash
Ross's Private Key
3
A#13%&23Rwe
Documents
Document + Encrypted Hash
Rachel's Public Key
4
Rachel's Private Key
Public Key Cryptography
5
A#13%&23Rwe
Documents
Ross's Public Key
6
334D016F755CD 136DC58C5F8E
Decrypt the Hash
Ross
Rachel
Documents
334D016F755CD 136DC58C5F8E
Hash of the Doc
Hash Function
1
Ross creating the Hash of the Document
7
Documents
334D016F755CD 136DC58C5F8E
Hash of the Doc
Hash Function
Rachel creating the Hash of the Document
8
334D016F755CD 136DC58C5F8E = 334D016F755CD 136DC58C5F8E
Rachel matching the Hashes
Hashes Matched ✓

Fig. 5. Digital signature for the given example (Rashmi Karan 2023)

3) *Characteristics of Blockchain*

i. *Decentralization:* In conventional centralized transaction systems, each transaction needs to be validated through a central trusted agency (eg: the central bank), inevitably resulting to the cost and the performance bottlenecks at the central servers. Contrast to the centralized mode, third party is no longer a necessity in blockchain.

ii. *Anonymity:* Each user can interact with the blockchain with a generated address, which does not reveal the real identity of the user.

iii. *Persistency:* Transactions can be verified quickly and invalid transactions would not be admitted by honest miners. It is not possible to delete or rollback transactions once they are included in the chain. Blocks that contain invalid transactions can be found instantly.

iv. *Auditability:* Bitcoin blockchain stores data about user balances based on Unspent Transaction Output (UTX-O) model [2]: Any transaction has to refer to some previous unspent transactions. Once the current transaction is recorded into the blockchain, the state of those referred unspent transactions change from unspent to spent. Thus, making it easy for the transactions to be tracked and verified.

4) *Gradation of the blockchain systems*

Currently, blockchain systems are categorized into three types: public, private and consortium [17]. In public blockchain, all records are visible to the public and everyone can take part in the consensus process. Unlike the consortium blockchain, where only a group of pre-selected nodes would participate in the consensus process. While, only those nodes that come from one specific organization would be allowed to join the process of consensus in a private blockchain.

A private blockchain is regarded as a centralized network because it is fully controlled by one singe organization. The consortium blockchain is partly decentralized as only a small portion of nodes would be selected to dedicate to the consensus. The comparison has been listed in table 1.

i. *Consensus determination:* In public blockchain, each node could take part in the consensus process and only a specific set of nodes are responsible for verifying the block in consortium blockchain. As for private chain it is fully controlled by one organization and the organization can determine the final consensus.

ii. *Read permission:* Transactions in a public blockchain are visible to the public. When it comes to private or consortium it depends on the consensus.

iii. *Immutability:* Records are stored in large number of participants, making it impossible to tamper transactions in a public blockchain. While in a private blockchain or consortium blockchain, the transactions could be tampered easily as there are only a limited number of seats of participants.

iv. *Efficiency:* It takes time to propagate transactions and blocks as there are a huge number of nodes on public blockchain network. As a result, transaction throughput is limited and the latency is high. With fewer verifiers, consortium and private blockchain could be more efficient.

v. *Centralized:* Major difference among the three types is that the public blockchain is decentralized, private is fully centralized and the consortium is partially centralized.

vi. *Consensus process:* Everyone in the world could join the process for a public blockchain. Otherwise, the other two types are invite-only or permission based.

Since public blockchain is open to the world, it can attract many consumers and communities. Many public blockchains emerge day by day. As for consortium blockchain, it is applied into many business applications. Currently Hyperledger [18] is developing business consortium blockchain framework systems. Ethereum has also provided tools for building these consortium blockchains [19].

D. *Consensus Algorithm*

1) *Approaches to consensus*

i. PoW (Proof of work): It is a consensus strategy used in bitcoin network. In a decentralized network, someone has to be selected to record the transactions. The simplest way is random choice. However, this might be vulnerable to attacks. Thereby, if a node wants to publish a block of transactions, a lot of work has to be done to prove that the node is not likely to attack the network. Usually, the work means computer calculations. In PoW, each node of the network is calculating value of the block header. The block header contains a nonce and miners would change the nonce frequently to get different hash values.

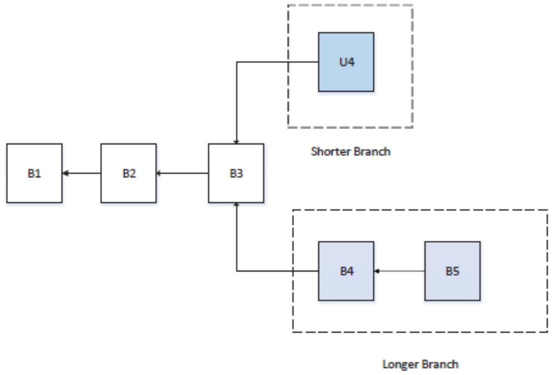

Fig. 6. Blockchain branches (T. Vijayakumar 2018)

The consensus needs the calculated value to be equal or smaller than a certain provided value. When one node reaches the target value, it broadcasts the block to other nodes and all other nodes must confirm the correctness of the hash value. If the block is verified, other miners would append this new block to their own chains. Nodes that calculate the hash values are called miners and the PoW procedure is called mining.

In the decentralized network, verified blocks might be generated simultaneously when multiple nodes find the suitable nonce at the same time approximately. Therefore, branches may be generated (Fig. 6). However, it is unlikely that two competing forks will generate next block at the same time. In PoW protocol, a chain that becomes longer thereafter is judged as the authentic one. Consider two forks created by verified blocks T4 and C4 at the same time. Miners keep mining their blocks until a longer branch is found. C4, C5 forms a longer chain, making miners on the T4 switch to the longer branch.

Miners have to do a lot of computer calculations in PoW, yet these works waste too much resources. To solve this loss, some protocols of PoW in which works could have some side-applications have been dedicatedly designed. For example, Primecoin [25] searches for special prime number chains which can be used for mathematical research.

ii. PoS (Proof of stake): It is an energy saving alternative to PoW. Miners in PoS have to prove the ownership of the amount of currency. It is observed that people with more currencies are less likely to attack the network. The selection based on account balance is quite unfair because the single richest person is bound to be dominant in the network. Consequently, many solutions are proposed with the compilation of the stake size to declare which one to forge the next block. Specifically, Blackcoin [26[uses randomization to predict the next generator. It uses a formula that looks for the lowest hash value in combination with the size of the stake. Peercoin [21] favours coin age based selection. In Peercoin, older and bigger sets of coins have a greater probability of mining the next block. Compared to the PoW, this saves more energy and is more effective. Unfortunately, the mining cost is almost zero here: making attacks as an easy consequence. Many blockchains adopt PoW at the starting and transform to PoS gradually. For example, Ethereum is planning to move from Ethash [27] to Casper [28].

iii. PBFT (Practical byzantine fault tolerance): This is a replication algorithm to tolerate byzantine faults [29]. Hyperledger Fabric [18] utilizes the PBFT as it consensus algorithm since it can handle up to $1/3^{rd}$ malicious byzantine replicas. A new block is determined in a round. In each round, a primary would be chosen according to some rules, responsible for ordering the transaction. The whole process is done in three parts: pre-prepared, prepared and commit. In each part, a node would enter the next part if it has received votes from over $2/3^{rd}$ of all nodes. Thus, PBFT needs every node to be known to the network. Stellar Consensus Protocol (SCP) [30] is also a byzantine agreement protocol like PBFT. In PBFT each node has to query other nodes while SCP gives participants the right to choose which set of other participants to believe. Based on PBFT, Antshares [31] has implemented their dBFT (delegated byzantine fault tolerance). In dBFT, some professional nodes are voted to record the transactions.

iv. DPOS (Delegated proof of stake): The major distinguished feature between PoS and DPOS is that PoS is direct democratic while DPOS is representative democratic. Stakeholders elect their delegates to generate and verify the blocks. With significantly fewer nodes to verify the block, the block could be confirmed faster, leading to the quick confirmation of transactions. Meanwhile, the parameters of the network such as block size and block intervals could be tuned by the delegates. Further users need not worry about the dishonest delegates as they could be voted out easily. DPOS is the backbone of Bitshares [22].

v. Ripple: This is an algorithm that utilizes collectively trusted subnetworks within the larger network. In the network, nodes are disciplined into two types: server for participating consensus process and client for only transferring funds. Each server has an Unique Node List (UNL). This is significant to the server. When deciding whether to put a transaction into the ledger, the server queries the nodes in UNL if the received agreements have reached 80%. The transaction would be packed into the ledger. For a node, the ledger remains corrected as long as the percentage of faulty nodes in UNL is not more than 20%.

vi. Tendermint [24]: This is again, a byzantine consensus algorithm. A new block is determined in a round. A proposer would be selected to broadcast an unconfirmed block in this round. It is disciplined in three steps:

1. Pre-vote step: Verifiers choose whether to broadcast a prevote for the proposed block.
2. Pre-commit step: If the node has received more than 2/3rd of pre-commits, it enters the commit phase.
3. Commit step: The node verifies the block and broadcasts a commit for that block. If the node has received 2/3 of the commits, it accepts the block

In contrast to PBFT, nodes have to lock their coins to become verifiers. Once a verifier is found to be dishonest, it would be punished.

2) *Consensus algorithms collation*

Different consensus algorithms have different advantages and disadvantages. Table 2 gives a comparisons between different consensus algorithms.

i. Node identity management: This is critical in consensus mechanisms like PBFT, which requires the identification of each participant to appoint a primary for every cycle, and Tendermint, which necessitates recognizing validators to nominate a proposer each round. Conversely, in PoW, PoS, DPOS, and Ripple protocols, nodes have the liberty to join the network without restrictions.

ii. Energy efficiency: PoW protocols demand substantial electrical power due to the continuous hashing of the block header to achieve a specific target value, leading to significant energy consumption. On the other hand, PoS and DPOS mechanisms, though still requiring the hashing of the block header, have considerably reduced energy requirements because the search space is intentionally limited. In contrast, PBFT, Ripple, and Tendermint eliminate the mining process in their consensus mechanism, resulting in substantial energy savings.

iii. Tolerated power of adversary: A common benchmark is the 51% hash power threshold, which, if exceeded, allows an entity to dominate the network. However, in PoW systems, a strategy known as selfish mining [10] enables miners to increase their profits with as little as 25% of the total hashing power. PBFT and Tendermint are engineered to withstand up to one-third of faulty nodes, while Ripple ensures operational integrity as long as less than 20% of nodes in an UNL are faulty.

iv. For illustrative purposes, Bitcoin employs PoW for its consensus mechanism, whereas Peercoin represents a peer-to-peer cryptocurrency that utilizes PoS. Hyperledger Fabric adopts PBFT for consensus, while Bitshares, a smart contract platform, opts for DPOS. Ripple and Tendermint, on the other hand, implement the Ripple protocol and the Tendermint protocol, respectively.

It's worth noting that PBFT and Tendermint are permissioned protocols, requiring known node identities within the network, making them more suited for commercial applications rather than public use. In contrast, PoW and PoS are more aligned with public blockchain environments. Consortium or private blockchains may prefer PBFT, Tendermint, DPOS, and Ripple due to their specific characteristics and requirements.

3) *Advancement on consensus algorithms*

In the realm of blockchain technology, the efficacy, security, and user-friendliness of consensus algorithms are paramount. Recent efforts have been directed towards refining these algorithms to address particular challenges inherent in blockchain systems. Innovations in consensus mechanisms are being developed with the goal of overcoming specific obstacles encountered within the blockchain framework. A notable innovation, PeerCensus [33], introduces a separation between the processes of block creation and transaction verification, thereby markedly enhancing the speed of achieving consensus. Furthermore, Kraft [34] has introduced an innovative consensus approach designed to regulate the pace of block generation, ensuring a more consistent output rate. This is a critical advancement given the recognition that an elevated rate of block generation can undermine the security framework of systems like Bitcoin.

The introduction of the Greedy Heaviest-Observed Sub-Tree (GHOST) chain selection principle [35] addresses these security concerns by deviating from the traditional longest branch methodology. Instead, GHOST evaluates the weight of different branches, allowing miners to opt for the most robust branch. This method significantly ameliorates the security

Table 2
Differentiation between typical consensus algorithms

Property	PoW	PoS	PBFT	DPOS	Ripple	Tendermint
Node ID management	open	open	permissioned	open	open	permissioned
Energy saving	no	partial	yes	partial	yes	yes
Tolerated power of adversary	<25% computing power	<51% stake	<33.3% faulty replicas	<51% verifiers	<20% faulty nodes in UNL	<33.3% byzantine voting power
Example	Bitcoin	Peercoin [21]	Hyperledger [18]	Bitshares [22]	Rippled [23]	Tendermint [24]

vulnerabilities associated with rapid block generation. Additionally, Chepurnoy et al. [36] have unveiled a novel consensus algorithm tailored for peer-to-peer blockchain networks. This algorithm permits individuals who furnish non-interactive proofs of retrievability concerning historical state snapshots to participate in block generation. This innovative approach necessitates that miners maintain only previous block headers rather than the entirety of full blocks, streamlining the storage requirements for participants in the blockchain network.

These advancements underscore the dynamic and evolving nature of consensus algorithms within the blockchain domain, highlighting the continuous pursuit of optimized efficiency, enhanced security measures, and improved accessibility for users across the blockchain ecosystem.

E. Future Directions of the Technology

The blockchain technology has demonstrated significant promise in both commercial and academic sectors. This text explores potential future developments in four distinct areas: testing of blockchains, addressing the issue of centralization, leveraging big data analytics, and broadening blockchain applications.

1) Examination of Blockchain Systems

With the emergence of numerous blockchain platforms and over 700 digital currencies listed as of now [52], the authenticity of claimed blockchain performance by some developers, driven by substantial profits, could be questionable. Furthermore, businesses looking to integrate blockchain into their operations must identify which blockchain technology aligns with their needs, necessitating a robust mechanism for blockchain evaluation.

The process of blockchain evaluation can be divided into two stages: the standardization and the testing phases. The standardization phase involves establishing and agreeing upon specific criteria. Following this, a blockchain can undergo testing based on these criteria to verify its functionality as per the developers' claims. During the testing phase, the evaluation should consider various metrics. For instance, an online retail business operator would be interested in the blockchain's throughput, necessitating tests on the average time it takes for transactions to be processed and included in the blockchain, the capacity of a blockchain block, among other aspects.

2) Addressing Centralization Concerns

Despite its decentralized design, blockchain has witnessed a trend towards miner centralization within mining pools. Currently, the five largest mining pools collectively control more than 51% of the total hashing power in the Bitcoin network [53]. Additionally, strategies like selfish mining [10] reveal that pools commanding over 25% of the total computational power can secure higher revenues than their fair share, potentially drawing rational miners to these pools until they surpass 51% of total power. To preserve blockchain's decentralized ethos, innovative solutions are needed to counteract this centralization.

3) Integration with Big Data

The synergy between blockchain and big data presents two main opportunities: data management and analytics. Blockchain's distributed and secure nature makes it an ideal platform for storing critical data, ensuring its authenticity and protection. For instance, utilizing blockchain for patient health records could safeguard against tampering and unauthorized access. On the analytics front, blockchain transaction data could facilitate big data analysis, such as identifying trading patterns, enabling predictions about potential partners' trading behaviours.

4) Expanding Blockchain Usage

While blockchain is predominantly used in finance, its application is expanding across various sectors. Traditional industries are encouraged to explore blockchain to enhance their systems, such as implementing blockchain for user reputation management. Emerging industries can also benefit from blockchain to boost efficiency, as seen with Arcade City [51], a ridesharing startup that uses blockchain for a direct connection between riders and drivers.

Smart contracts represent a significant innovation within blockchain. Defined as automated transaction protocols that fulfil contract terms [54], smart contracts were conceptualized long ago and are now executable on blockchain platforms. These code snippets, run by miners, hold the potential to revolutionize sectors like financial services and the Internet of Things (IoT) through automation and enhanced security.

5. Homomorphic Encryption

A. Understanding of homomorphic encryption

The studies of homomorphic encryption techniques have led to significant advancements in the computing domain. It provides a means for securely transmitting and storing confidential information across and in a computer system.

Webster’s dictionary defines homomorphism as a “mapping of mathematical set into or another set or itself in such a way that the result obtained by applying operations to elements of the first set is mapped onto the result obtained by applying those corresponding operations to their respective images in the second set” [73]. The word homomorphism derives from the Greek word homos meaning “same” and morphe meaning “shape”. In computer science, this is used in conversion of plain text to ciphertext.

Plaintext refers to any information that a sender desires to transfer to a receiver. It can be thought of as an input to any algorithm or as information being transmitted before an algorithm encrypts it. For instance, email messages, word processor files, images, or ATM and credit card transactions are plaintexts. The plaintext is converted into ciphertext which is the data that has been encrypted and is unreadable until it has been decrypted with a key.

Homomorphic encryption seeks to aid in this encryption process by allowing specific types of computations to be carried out on ciphertext which gives an encrypted result which is also in ciphertext. Its outcome is the result of operations performed on plaintext. One person could add two encrypted numbers and then another person could decrypt the result, without either of them being able to find the value of the individual numbers.

If a consumer wishes to process confidential data onto another person's computer, which is a server in the cloud and wants to ensure that no one else gains access to that data, including the owner of the computer, conventional methods of encryption would protect their data while it is in transit, but not while the computation is going on. This provides security to the consumers' information from the moment data stream leaves their computer until it returns. This method requires that all the arithmetical and logical operations needed in the computation, which may be represented by circuits or gates, be applied to encrypted form of the data [74].

B. Significance

In April 2011, Sony's PlayStation network was hacked into and millions of consumers' accounts were breached leaking credit card information, physical addresses, passwords and other personal information [75]. Sony accepted its own responsibility and mishandling for the incident admitting that they could have taken special precautions by encrypting the data on their network. Around the same time, researched discovered that Dropbox was storing unencrypted files of consumers. As a result, consumers closed their accounts in protest angry at the company for not encrypting their confidential files [76].

The solution to this predicament these two companies faced was not as conspicuous as one might assume. Firstly, in order for data to have been used by their consumers and clients, the data had to be decrypted. To do so, the decryption key had to be located somewhere between the data storage and the consumer. However, this was extremely tedious to achieve without jeopardizing the security of the client's data. For example, Sony required to be able to charge their customers credit card whether they were online or not and this required a billing address. Even if card numbers and addresses were encrypted, the need to store the decryption key somewhere on their servers still existed. If they offered an "update account: page with the address pre-filled, the decryption key had to be available to decrypt the data as soon as the consumer clicked the update my account button [76]. Therefore, if Sony's web servers need to be able to decrypt data, and hackers hack into Sony's servers, there is only so much protection encryption would have been able to provide. The development of cloud storage systems such as dropbox and computing platforms gives consumers the ability to outsource storage and computations on their data. Further allows businesses to outsource an ascending amount of data storage and management to cloud services. Although they profit these advantages, the potent drawbacks of handling with these predicaments along with Sony's issues is to encrypt all the data stored in the cloud and perform operations on encrypted data. If the encryption scheme is homomorphic, the cloud can still perform meaningful computations on the data, even though its encrypted [77].

C. Mannerism of Homomorphism Theoretically

Earlier, homomorphic encryption was defined as a form of encryption where a specific algebraic operation performed on plaintext is equivalent to another algebraic operation performed on its ciphertext. In mathematics, these operations are called functions and are operation preserving mappings (OP mappings). For instance, if (A,0) and (B,*) represent groups, an OP mapping b(A,0)→(B,*) is called a homomorphism from (A,0) to (B,*). The groups represent sets of data and the mapping or the function that maps the set (A,0) onto or into the set (B,*) and is denoted as h [78]. This function is an operation that preserves the structure from one set of data to another set of data.

Mathematical analogies can be utilized to explain the concepts behind homomorphic encryption. The succeeding explanation and illustration in this section has been adopted from Briayn Hayes' Alice and Bob in Cipherspace article in the American Scientist Journal.

To further explain how homomorphism works, we consider two sets of data. One is the set of positive real numbers R+ and the other set is the logarithms of this set of real numbers. On these sets, the multiplication of real numbers and the addition of logarithms are homomorphic encryptions. If we consider any real positive numbers a,b and c. if a•b=c, then log(a)+log(b) = log(c). This gives us with two alternate paths for obtaining our result c. For the first method, if we are provided with a and b, we can multiply them together to obtain c. As the second option, we can add the logarithms of a and b and take the antilog of the sum to arrive at c. Both the cases produce the same conclusion [74]. With homomorphic encryption we can perform arithmetic directly on the plaintext inputs a and b. Or we can encrypt a and b, apply a series of operations to ciphertext values, then decrypt to result to arrive at the same final answer. The two routes pass through parallel universes: plainspace and cipherspace.

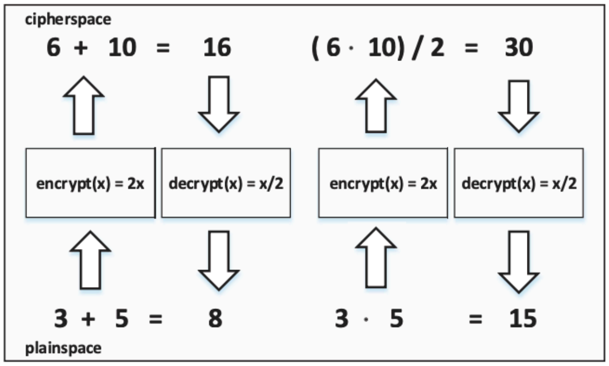

Fig. 7(a). Example of encryption of numerical values as plaintext using homomorphic encryption

In Figure 7(a), two distinct collections of numerical entities are depicted, with the lower cluster encompassing the complete set of integers, denoted by Z, while the upper cluster is indicative of the subset comprising solely even integers. The mathematical operations applied to these entities are those of addition and multiplication. The procedure of transitioning between these two collections involves either the doubling or halving of a numerical value. With respect to the operation of addition, the integers 3 and 5 serve as the original, unencrypted inputs. These figures undergo encryption through a process of doubling, thus transforming into the values 6 and 10, respectively. Within the encrypted realm, termed cipherspace, these altered values are then subject to addition, culminating in the sum of 16. To revert to the original, meaningful value, the resulting encrypted sum is decrypted by a factor of 2, leading to the final outcome. Adjacently, a similar but distinct example elucidates the methodology for multiplication. Utilizing the same unencrypted starting points of 3 and 5, these numbers are likewise encrypted by a factor of 2. However, to derive the multiplication result of these original values, the product of their encrypted counterparts is then halved.

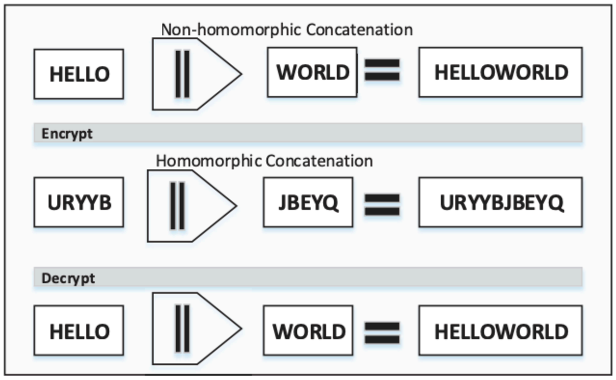

Fig. 7(b). Example of concatenation of two words using homomorphic encryption

Figure 7(b) presents a case study on the application of homomorphic encryption for the purpose of joining two separate strings of text. In this particular instance, the operation that fuses the plaintext words HELLO and WORLD is replicated to merge their encrypted equivalents. It is important to note that such a parallel in operations between plaintext and ciphertext is not a given in all scenarios. The essential insight here is that it's possible to execute a certain operation on the encrypted inputs, which yields a new form of encrypted data. When this new ciphertext is decrypted, it reveals a plaintext that is the result of the originally intended operation performed on the initial plaintext inputs, as cited in reference [79].

Delineating on the three pivotal encryption frameworks which must be highlighted are Partially Homomorphic Encryption (PHE), Somewhat Homomorphic Encryption (SWHE), and Fully Homomorphic Encryption (FHE). PHE allows the execution of a singular type of operation on ciphered data, for example, either multiplication or addition, but not concurrently. On the other hand, SWHE extends this capability slightly further by facilitating a finite sequence of both addition and multiplication operations on encrypted data. In contrast, FHE represents a more advanced scheme that supports unlimited operations of both addition and multiplication, enabling the computation of any arbitrary function on encrypted data.

The utilization of FHE is particularly valuable because it enables the homomorphic evaluation of circuits. This allows for the creation and execution of algorithms that can operate on encrypted inputs to yield an encrypted output. The remarkable aspect of such algorithms is their ability to function without ever decrypting the inputs, thus preserving confidentiality even when processed by entities that cannot be considered entirely secure.

However, it's pertinent to acknowledge that PHE and SWHE still hold a competitive edge over FHE in terms of efficiency. Despite the expansive capabilities of FHE, PHE and SWHE systems are currently more efficient in processing operations on encrypted data.

Most of the current encryption schemes that can be feasily used on cloud services are somewhat or partially homomorphic. Microsoft researchers, Kristin Lautner, Vinod Vaikuntanathan and Michal Naehrig developed a prototype that demonstrates a somewhat homomorphic encryption technique. Their technique allows addition and a few multiplications to be done on encrypted data, which in turn allows them to perform simple functions on the ciphertext in the domain of statistics. The computations used may calculate averages and compute standard deviations or perform other operations such as logical regressions which can be used to predict the likelihood of specific health issue [77].

These researchers are optimistic about utilizing SWHE scheme as a fundamental base for developing an applicable FHE technique in the near future. The implementation of these types of encryption on a large scale data sets have also been looked into. A method for computing the mean and variance of univariate and multivariate data as well as performing linear regression on multidimensional encrypted data already has been legislated [80].

These types of encryption techniques are continuing to progress and evolve. It has been claimed numerous times that homomorphic encryption will need further developments before companies will become interested in its usage. The encrypted data can be pushed into a cloud service today but it cannot be indexed, searched or operated on [81]. These are some of the most desired or applied operations onto data sets today, and at the same time they are current limitations too.

D. Current Studies

In his seminal doctoral thesis of 2009, Craig Gentry introduced the pioneering fully homomorphic encryption (FHE) scheme, which was revolutionary in enabling the execution of arbitrary computations on ciphered data without necessitating the decryption key [82]. Gentry's initial approach was to construct a somewhat homomorphic encryption scheme and then simplify the associated decryption circuit, thus setting the foundation for a bootstrapped FHE scheme.

Advancing this field further, in 2011, Craig Gentry, in collaboration with Shai Halevi, developed an enhanced technique by amalgamating SWHE with multiplicatively homomorphic encryption (MHE). This innovative strategy effectively obviated the need for the previously essential compression step introduced in Gentry's dissertation. Their refined method was successful in compressing the FHE ciphertexts into a singular, more secure ciphertext. This modified technique still employed bootstrapping but circumvented the need to simplify the decryption circuit [82].

Over the past year, there has been considerable progress in refining FHE methods. Despite this, the challenge of inefficiency remains, as current implementations are not sufficiently efficient for widespread practical application [83]. To address this, Gentry, together with researchers Halevi, Peikert, and Smart, investigated ways to optimize homomorphic computations on lower levels of computational circuits by reducing the size of the polynomial rings used. A ring homomorphism, within the realm of ring theory or abstract algebra, is a mapping that retains the ring operations of addition and multiplication. Their research focused on converting ciphertexts from a larger polynomial ring to a smaller one while preserving the encrypted data, a process termed 'ring switching.' They employed a polynomial reduction strategy that decomposes a high-degree polynomial into multiple polynomials of lower degrees. The rationale was to ensure that the original data, encrypted in a large-ring ciphertext, could be accurately retrieved as a straightforward linear combination of the data encrypted in the small-ring ciphertexts. The ultimate aim of this ring switching process was to transmit ciphertexts of reduced size, thereby enhancing the efficiency of the FHE system [84].

E. Applicative Example to Explain the Working of Homomorphic Encryption

To demonstrate a practical utility for this technique, an algorithm that models this process was developed by researchers Monique Ogburna, Claude Turnerb, Pushkar Dahal. A scenario where a hospital outsources the patients' information to a contracting company has been taken in consideration. The hospital encrypts this information and forwards this data to the contractor whose purpose is to determine the patient(s) with high BP. Once the agency decrypts the person's name; no need to provide the contractor with the key. This process has been elaborated in Fig. 8.

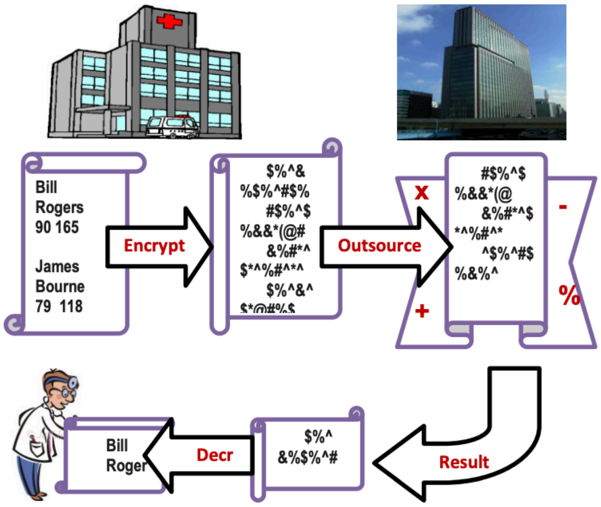

Fig. 8. Outsourcing encrypted data to contractor

Because the blood pressure is declared as integers, the ASCII value will also be integer; this allows to perform comparison operations such as greater than or less than on the encrypted data. This might not always be the case depending on the parameters of the scheme of encryption and the encryption key preferred. This program outputs the names associated with values. No comparison operations are performed on the names, only on numerical BPs. Although the encryption function is not the most robust function, this instance illustrates the potent for implementing a homomorphic encryption method. While the data set used in this case is a small set, the use of homomorphic encryption schemes can be extended to sets containing a sizeable amount of information. Experiments have been conducted on large sets of encrypted data to perform linear regressions and calculate the variance and mean of that data. In these experiments the number of data points ascend up to four million elements and one million elements respectively [80].

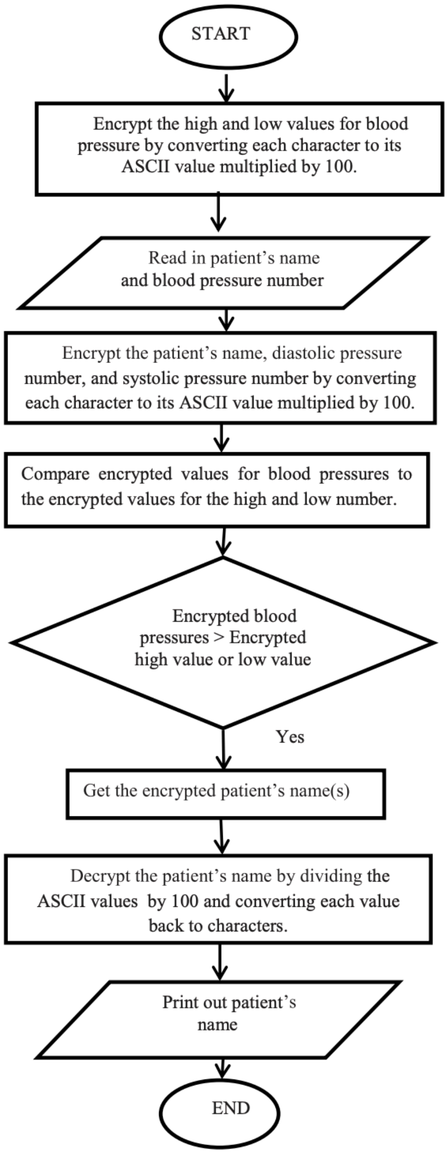
START
Encrypt the high and low values for blood pressure by converting each character to its ASCII value multiplied by 100.
Read in patient's name and blood pressure number
Encrypt the patient's name, diastolic pressure number, and systolic pressure number by converting each character to its ASCII value multiplied by 100.
Compare encrypted values for blood pressures to the encrypted values for the high and low number.
Encrypted blood pressures > Encrypted high value or low value
Yes
Get the encrypted patient's name(s)
Decrypt the patient's name by dividing the ASCII values by 100 and converting each value back to characters.
Print out patient's name
END

Fig. 9. Homomorphic algorithm

F. Other Applications in real life

1) Medical industry

Historically, there have been suggestions for the utilization of private cloud-based systems for the storage of medical records, known as Patient Controlled Encryption. In such a system, a patient's medical data is first encrypted by healthcare practitioners before it is transferred to the patient's personal cloud storage. Control over who can access these medical records rests with the patient, who can grant access by distributing secret keys to chosen healthcare entities. This setup allows patients and authorized entities to perform searches within the encrypted records. However, one limitation is that the cloud service is restricted to simple search functions and cannot execute any other form of computation on the encrypted data [77]. The integration of Fully Homomorphic Encryption (FHE) would empower the cloud system to conduct various operations on the encrypted data for the benefit of the patient. For example, if monitoring devices continuously relay health-related data to the cloud, implementing FHE would allow the cloud to process this encrypted data and then relay updates, notifications, or other critical information back to the patients. Encrypted data that might be processed in such a manner could include sensitive information like blood pressure levels, glucose concentrations, patient ages, and other medical details that patients and their healthcare providers consider confidential.

2) Financial industry

In the realm of finance, the protection of sensitive information is paramount for both clients and companies. It is essential that the data and the computations performed on it remain confidential. For example, information regarding company profiles, fluctuations in stock prices, or inventory levels can be critical in formulating investment strategies. This data may be delivered continuously, providing the latest insights crucial for making informed trading decisions [77]. Consequently, the algorithms used to process this data must be proprietary. Such algorithms could encompass novel predictive models for forecasting stock prices, often derived from the costly and extensive research carried out by financial experts. Understandably, firms are inclined to safeguard these valuable models to maintain a competitive edge and secure their research investments. Incorporating a fully homomorphic encryption (FHE) technique could allow for the private evaluation of these functions. For instance, a client could safely transmit an encrypted variant of the function to a cloud service, which could include a program with certain computations using encrypted inputs. Additionally, data streams could be encrypted with the client's public key and sent to the cloud. The cloud provider could then execute the confidential function using the encrypted program's specification on the received encrypted data. Once computed, the cloud would relay the encrypted result back to the client, ensuring that sensitive information remains secure throughout the process [77].

6. Blockchain Technology in the AA System

A. Benefits of Blockchain in AA System

1) Enhanced Security

Blockchain technology can significantly enhance the security of the Account Aggregator (AA) system through its inherent cryptographic protection and decentralized nature. In a blockchain-based AA system, each transaction and data exchange is encrypted and recorded across multiple nodes in the network, making it nearly impossible for unauthorized parties to alter the data. This decentralization eliminates single points of failure, drastically reducing the risk of cyber-attacks and data breaches that are more common in centralized systems. The security of blockchain ensures that sensitive financial information remains confidential, only accessible by parties who are granted explicit permission, thereby safeguarding user data against unauthorized access and fraud. This level of security is paramount in financial systems, where trust and data integrity are crucial. By leveraging blockchain, the AA system can offer a more robust framework for data sharing, instilling greater confidence among users and participating entities.

2) Improved Data Privacy

Blockchain's approach to data privacy is fundamentally different and more secure than traditional data handling methods. In a blockchain-based AA system, data privacy is enhanced through the use of permissioned ledgers and cryptographic techniques that ensure data is shared only with consent and remains inaccessible to unauthorized parties. Users can have granular control over who accesses their data, under what circumstances, and for how long, using digital keys and smart contracts. This not only puts power back into the hands of the users but also ensures compliance with strict data protection regulations. The ability to verify transactions without exposing underlying data to the validators is a cornerstone of blockchain privacy features, enabling secure and private verification of financial transactions. This level of control and privacy is particularly important in the financial sector, where personal and sensitive data must be protected from misuse and unauthorized access.

3) Increased Efficiency

Blockchain technology can streamline many of the operational processes within the AA system through automation and the elimination of intermediaries. Smart contracts, self-executing contracts with the terms of the agreement directly written into code, can automate the consent and data-sharing process, significantly speeding up transactions while reducing the potential for human error. This automation can lead to a more efficient operational model, as transactions on the blockchain can occur 24/7 without the need for manual processing. Moreover, blockchain's distributed ledger technology allows for real-time data sharing and reconciliation, eliminating the delays and discrepancies that often occur in traditional systems. The efficiency gains from blockchain can reduce operational costs for financial institutions and improve the user experience for customers, making financial services more accessible and convenient.

4) Greater Transparency

The immutable nature of blockchain technology ensures that every transaction and data exchange within the AA system is recorded on a ledger that cannot be altered retroactively. This creates an enduring and verifiable record of all interactions, enhancing transparency and trust among all participants. In a blockchain-based AA system, stakeholders can have access to a shared, transparent view of transaction histories and data exchanges, subject to their permissions, enabling greater accountability and trust. This level of transparency is particularly beneficial in financial ecosystems, where the clarity of transactions and data exchanges can help prevent fraud, errors, and misunderstandings. Moreover, the transparent nature of blockchain can facilitate regulatory oversight and compliance, as regulators can be granted access to view transactions in real-time, ensuring that all activities comply with relevant laws and regulations.

5) Interoperability

One of the key benefits of implementing blockchain in the AA system is the potential for enhanced interoperability among diverse financial institutions and fintech applications. Blockchain platforms can provide a standardized protocol for secure and efficient data exchange, enabling different systems to communicate with each other more effectively. This interoperability is crucial for the seamless functioning of the AA system, as it involves multiple stakeholders, including banks, non-banking financial companies (NBFCs), and fintech services. By using blockchain as a common framework, these entities can share data more easily and securely, without the need for costly and complex integration efforts. This not only improves the user experience by providing a more cohesive financial ecosystem but also fosters innovation by allowing for the development of new services and applications that can easily interact with existing infrastructure.

B. Implementation Strategy

1) Assessment and Planning

Implementing blockchain technology in the AA system starts with a comprehensive assessment and planning phase. This involves a detailed analysis of the current system to identify processes and areas where blockchain can add value, such as data sharing, consent management, and transaction processing. It's essential to understand the specific needs of the AA system, including regulatory requirements, stakeholder expectations, and technical challenges. The planning phase should result in a strategic roadmap that outlines the goals, timelines, and milestones for the blockchain implementation, including pilot projects, full-scale deployment, and future expansions. This phase requires collaboration among technology experts, financial industry stakeholders, and regulatory bodies to ensure the proposed blockchain solution aligns with all operational, legal, and business objectives. Effective assessment and planning set the foundation for a successful blockchain integration, addressing potential hurdles and aligning expectations across the board.

2) Platform Selection

Choosing the right blockchain platform is critical for the success of integrating blockchain into the AA system. The selection process should consider various factors, including the platform's scalability, consensus mechanism, privacy features, and ease of use. Scalability is crucial to ensure the system can handle the volume of transactions and data exchanges typical in financial services. The consensus mechanism affects the speed and security of transactions, while privacy features are essential for protecting sensitive financial data. Additionally, the platform should have a supportive developer community and comprehensive documentation to facilitate development and troubleshooting. It's also important to consider interoperability with existing financial systems and other blockchain networks. The chosen platform should align with the specific requirements of the AA system, balancing the need for security, efficiency, and regulatory compliance. Engaging with blockchain experts and conducting thorough research and testing are key steps in selecting the most suitable platform.

3) Pilot Program

Before a full-scale rollout, it's advisable to launch a pilot program to test the blockchain integration in a controlled environment. This allows for the identification of technical challenges, operational issues, and user experience aspects that need to be addressed. A pilot program can focus on a specific segment of the AA system, such as consent management or data sharing between a limited number of entities. This approach enables real-world testing of the blockchain solution, providing valuable insights into its performance, scalability, and security. Feedback from users and stakeholders during the pilot phase is crucial for refining the system and ensuring it meets the needs of all parties involved. Additionally, a successful pilot can serve as a proof of concept, demonstrating the benefits of blockchain integration to skeptical stakeholders and regulatory bodies. It's a critical step in building confidence and gaining the necessary support for a wider implementation.

4) Stakeholder Engagement

Engaging with stakeholders is a crucial component of the implementation strategy for integrating blockchain into the AA system. This includes financial institutions, regulatory authorities, technology providers, and end-users. Effective engagement ensures that the blockchain solution addresses the needs and concerns of all parties involved. It's important to establish clear communication channels and feedback mechanisms to gather input and keep stakeholders informed about the project's progress. Engaging with regulatory bodies from the outset is particularly important to ensure the blockchain solution complies with financial regulations and data protection laws. Collaboration with technology providers can leverage their expertise and resources, while feedback from end-users can help optimize the user experience. Building a coalition of supportive stakeholders can also facilitate smoother integration and adoption of the blockchain solution across the financial ecosystem.

5) Regulatory Compliance

Ensuring regulatory compliance is a critical aspect of implementing blockchain in the AA system. Financial services are highly regulated, and any new technology must adhere to existing laws and regulations concerning data protection, consumer rights, and financial transactions. Early engagement with regulatory bodies can provide clarity on regulatory expectations and identify any potential compliance issues. It may also be necessary to advocate for regulatory adjustments or clarifications to accommodate the innovative aspects of blockchain technology. Compliance considerations should be integrated into the design and operation of the blockchain system, including data privacy, security measures, and transaction reporting. Working closely with legal and regulatory experts can help navigate the complex regulatory landscape, ensuring that the blockchain-enabled AA system operates within legal boundaries while leveraging the full potential of blockchain technology.

6) Technology Integration

Integrating blockchain technology into the existing AA infrastructure requires careful planning and execution. This involves developing APIs (Application Programming Interfaces) and smart contracts to facilitate seamless data exchange and automate processes within the blockchain network. Ensuring compatibility with existing financial systems and protocols is crucial for a smooth integration process. This may involve adapting or upgrading current systems to work efficiently with blockchain technology. The integration process should be conducted in phases, allowing for testing and adjustments as needed. Strong technical support and clear documentation are essential to resolve issues and ensure that all participants can connect and interact with the blockchain system effectively. Successful technology integration not only enhances the functionality and efficiency of the AA system but also lays the foundation for future innovations and services.

7) Training and Support

Providing training for users and technical support teams is essential to ensure they are equipped to use and manage the blockchain-enabled AA system effectively. Training programs should cover the basics of blockchain technology, the specifics of the AA system's blockchain implementation, and the operational procedures for different user roles. This education is crucial for building confidence and competence among users, facilitating smoother transactions, and reducing errors. Technical support teams should be well-versed in troubleshooting and resolving issues related to the blockchain system, ensuring reliable operation and user satisfaction. Ongoing support and updates are necessary to address emerging challenges and incorporate advancements in blockchain technology. A well-designed training and support program can accelerate adoption, enhance user experience, and ensure the long-term success of the blockchain-enabled AA system.

C. Required Resources and/or Support

1) Technical Expertise

Implementing blockchain technology within the AA system requires a team of skilled blockchain developers and engineers. These professionals should have expertise in the selected blockchain platform, smart contract development, and the integration of blockchain with existing financial systems. They play a crucial role in designing, building, and maintaining the blockchain infrastructure, ensuring it meets the specific needs of the AA system. Recruiting or training staff with the necessary technical skills is a critical step in the implementation process. Additionally, collaboration with external blockchain experts and technology providers can supplement internal capabilities, providing specialized knowledge and experience. Building a strong technical team is essential for navigating the complexities of blockchain development and ensuring a successful implementation.

2) Regulatory Guidance

Navigating the regulatory landscape of financial services is a complex task that requires specialized knowledge and expertise. Legal and regulatory experts are essential resources for ensuring that the blockchain-enabled AA system complies with all applicable laws and regulations. These professionals can provide guidance on data protection, financial regulations, and consumer rights, helping to design a system that meets legal requirements while leveraging the benefits of blockchain technology. Engaging with regulatory bodies and staying informed about regulatory changes are crucial for maintaining compliance and advocating for regulatory environments that support innovation. Regulatory guidance is a critical resource for mitigating legal risks and building a blockchain system that is both innovative and compliant.

3) Financial Investment

Developing and implementing a blockchain solution for the AA system involves significant financial investment. Funding is required for technology development, infrastructure setup, pilot programs, and ongoing maintenance. This investment may come from various sources, including internal budgets, venture capital, government grants, or partnerships with financial institutions and technology providers. Securing adequate funding is crucial for covering the costs of technical development, regulatory compliance, training, and support. It also allows for the exploration of innovative features and services that can enhance the AA system. A well-planned budget and clear investment strategy are essential for ensuring the financial viability of the blockchain project.

4) Collaboration Tools

Effective collaboration among the diverse stakeholders involved in the AA system is essential for a successful blockchain implementation. Collaboration tools and platforms facilitate communication, project management, and document sharing among team members, financial institutions, regulatory bodies, and technology providers. These tools support the coordination of development efforts, regulatory compliance activities, and stakeholder engagement initiatives. Choosing the right collaboration tools can enhance efficiency, reduce misunderstandings, and ensure that all participants are aligned and informed throughout the project. Investing in robust collaboration infrastructure is key to managing the complex ecosystem of the AA system and achieving a cohesive implementation process.

5) Infrastructure

A robust IT infrastructure is essential for supporting the operations of a blockchain-enabled AA system. This includes hardware, such as servers and network equipment, and software, such as blockchain nodes, databases, and security systems. The infrastructure must be scalable to handle increasing volumes of transactions and data exchanges as the AA system grows. It should also be secure to protect sensitive financial information and ensure compliance with data protection regulations. Cloud services can offer flexibility and scalability, allowing the AA system to adapt to changing demands. Ensuring the reliability and performance of the IT infrastructure is crucial for the smooth operation of the blockchain system and the satisfaction of users and stakeholders.

D. Miscellaneous

1) Continuous Learning and Adaptation

The fields of blockchain and financial technology are rapidly evolving, with new advancements and regulatory changes occurring frequently. Continuous learning and adaptation are essential for keeping the blockchain-enabled AA system at the forefront of technology and compliance. Staying informed about technological developments, regulatory updates, and industry best practices can help identify opportunities for improvement and innovation. It's also important to be adaptable, ready to adjust strategies and technologies in response to new challenges and opportunities. Encouraging a culture of learning and innovation within the organization and among stakeholders can foster continuous improvement and ensure the long-term success of the AA system.

2) Community Building

Building a community of developers, users, and advocates around the blockchain-enabled AA system can drive innovation and collaboration. A strong community can provide support, share knowledge, and contribute to the development of new features and applications. Engaging with the wider blockchain and financial technology communities through forums, social media, and events can raise awareness of the AA system and attract talent and investment. Community feedback is invaluable for improving the system, identifying user needs, and exploring new use cases. Investing in community building efforts can enhance the ecosystem around the AA system, encouraging innovation and fostering a sense of ownership and commitment among participants.

3) Scalability and Future-Proofing

Designing the blockchain system with scalability in mind is crucial for accommodating future growth and evolving use cases within the AA ecosystem. The system should be able to handle increasing numbers of transactions, users, and data exchanges without compromising performance or security. This requires careful architectural planning, the use of scalable blockchain technologies, and the anticipation of future needs and challenges. Additionally, future-proofing the system involves staying adaptable to technological advancements, regulatory changes, and market trends. Ensuring the blockchain-enabled AA system is scalable and future-proof can support long-term growth and innovation, making it a robust and resilient platform for financial data sharing.

7. Homomorphic Encryption in the AA System

A. Benefits of Homomorphic Encryption in AA System

- Enhanced Data Privacy and Security: Homomorphic encryption is a game-changer for data privacy and security in the Account Aggregator system. It allows data to be encrypted in such a way that it can still be processed without ever being decrypted. This means that sensitive financial information remains secure even when being shared or analyzed. Traditional encryption methods require data to be decrypted for processing, creating vulnerabilities. However, with homomorphic encryption, data breaches and unauthorized access risks are significantly minimized because the data, even if intercepted, remains indecipherable. This technology ensures that the confidentiality and integrity of data are preserved, making it a robust solution for protecting sensitive financial information in an increasingly digital world.
- Regulatory Compliance: Adhering to regulations like GDPR in Europe or CCPA in California requires stringent data protection measures. Homomorphic encryption enables financial institutions within the AA ecosystem to process and analyze encrypted data without violating privacy laws. This is because the technology allows for the computation of encrypted data, ensuring that personal information remains confidential throughout the process. For regulators and institutions alike, this represents a significant step forward in maintaining privacy standards while still enabling the necessary data flow for financial services. It offers a pathway to leveraging big data analytics and AI in compliance with privacy laws, transforming how financial data is managed while upholding individuals' privacy rights.
- Secure Data Sharing: In the Account Aggregator framework, secure data sharing between entities is crucial. Homomorphic encryption allows for the sharing of financial data in an encrypted form, ensuring that only authorized parties can process and understand it. This level of security promotes collaboration and innovation among financial institutions, fintech companies, and other stakeholders by allowing them to utilize sensitive data without compromising its confidentiality. It essentially creates a secure environment for data sharing, where insights can be gained and services improved without exposing the raw data, thus fostering trust and cooperation in the financial ecosystem.
- Data Utility Preservation: One of the most compelling benefits of homomorphic encryption is its ability to preserve the utility of data while ensuring its privacy. Traditional encryption methods can protect data at rest or in transit but render it unusable for analysis without decryption. Homomorphic encryption, on the other hand, supports operations on encrypted data, enabling insightful analytics and processing without ever exposing the actual data. This means financial institutions can perform risk assessments, fraud detection, and personalized service offerings based on encrypted data, thereby maximizing data utility without compromising security or privacy.

B. Implementation Strategy

- Assessment and Planning: Implementing homomorphic encryption in the AA system starts with a thorough assessment of the existing infrastructure. This involves understanding the data flow, identifying sensitive data that needs encryption, and determining the processing operations to be performed on this data. Planning also requires setting clear objectives for what the implementation aims to achieve, such as compliance with specific regulations, enhancing data security, or enabling secure data sharing. This stage is crucial for laying the groundwork for homomorphic encryption integration, as it sets the direction for the technical and strategic decisions that follow.

- Select Homomorphic Encryption Scheme: The selection of a homomorphic encryption scheme is critical and depends on the specific needs of the AA system, such as the complexity of data processing tasks and the performance requirements. Fully Homomorphic Encryption (FHE) offers the most flexibility by supporting arbitrary computations on encrypted data but at the cost of significant computational overhead. Partially or Somewhat Homomorphic Encryption schemes, while more limited in the operations they support, can offer better performance. The choice of scheme should balance the desired level of security and computational efficiency, taking into consideration the current state of the technology and the specific use cases within the AA system.
- Integration with Existing Infrastructure: Integrating homomorphic encryption into the existing Account Aggregator infrastructure requires careful planning and execution. This involves modifying data processing workflows to incorporate encrypted data processing, which may include changes to data storage, transmission, and analytics processes. The integration strategy should ensure that the system remains functional and efficient while adopting the new encryption method. This may require updates to software, hardware upgrades, or even the development of new applications designed to work with encrypted data. Ensuring compatibility with existing systems while minimizing disruption to services is a key challenge during this phase.
- Pilot and Testing: Before full-scale implementation, conducting a pilot project is essential to test the homomorphic encryption solution within the AA system. This controlled environment allows for identifying any potential issues related to performance, compatibility, or security. The pilot phase is an opportunity to fine-tune the system, optimize performance, and ensure that the encryption does not adversely affect the system's functionality. Feedback from this phase can guide further adjustments and improvements, ensuring that the system is robust, secure, and ready for wider deployment.

C. *Required Resources*

- Expertise in Cryptography and Data Security: Implementing homomorphic encryption requires a team with specialized knowledge in cryptography and data security. These experts will be responsible for selecting the appropriate encryption scheme, integrating it with the existing infrastructure, and ensuring that the system remains secure against evolving threats. They will also play a crucial role in ongoing maintenance and updates to the encryption algorithms. Investing in skilled professionals is essential for the successful implementation and operation of a secure and efficient AA system powered by homomorphic encryption.
- Technology and Infrastructure: The computational demands of homomorphic encryption are significant, necessitating substantial investment in technology and infrastructure. This includes powerful computing resources capable of handling the encryption and decryption processes efficiently. For many organizations, this may mean upgrading existing hardware or moving to cloud-based solutions that can offer the required computational power. Additionally, software tools and platforms that support homomorphic encryption need to be developed or adapted, requiring further investment in technology and development resources.
- Regulatory and Compliance Advisory: Navigating the complex landscape of financial regulations and data protection laws is a critical aspect of implementing homomorphic encryption in the AA system. Legal and regulatory advisors can provide invaluable guidance on compliance matters, ensuring that the system meets all relevant requirements. This support is crucial for avoiding legal pitfalls and ensuring that the implementation does not inadvertently breach any regulations.
- Training and Education: The successful implementation of homomorphic encryption also depends on the awareness and understanding of the staff involved. Training programs designed to educate employees about the new system, its capabilities, and the best practices for handling encrypted data are essential. This not only ensures smooth operation but also helps in fostering a culture of security and privacy awareness within the organization.

D. *Miscellaneous*

- Performance Considerations: The primary challenge with homomorphic encryption is its impact on system performance due to the heavy computational load. Addressing this issue requires a multifaceted approach, including selecting the most efficient encryption schemes, optimizing algorithms, and leveraging hardware acceleration technologies. Cloud computing resources can also offer scalable solutions to meet the computational demands. It's crucial to balance the security benefits of homomorphic encryption with the practical considerations of system performance and user experience.

- Collaboration and Partnership: Advancements in homomorphic encryption and its application in the AA system can benefit greatly from collaboration with technology providers, academic institutions, and industry consortia. These partnerships can provide access to cutting-edge research, technological innovations, and best practices in the field. Collaborative efforts can also help in standardizing approaches and creating a more secure and interoperable ecosystem for financial data sharing and processing.
- Continuous Monitoring and Update: The digital security landscape is constantly evolving, with new threats emerging regularly. To maintain the integrity and security of the AA system, continuous monitoring for vulnerabilities and regular updates to the encryption algorithms are necessary. This proactive approach ensures that the system remains secure against new threats and continues to provide the highest level of data protection and privacy for users.

8. Conclusion

The integration of Blockchain technology and Homomorphic Encryption into India's AA system represents a significant leap forward in the nation's quest to establish a secure, efficient, and inclusive financial landscape. The allocation of the 2024 budget for technology and financial inclusion initiatives underpins the government's staunch commitment to fostering innovation and accessibility in the sector, ensuring that the advantages of digital transformation are equitably distributed across the country. Blockchain technology, celebrated predominantly for its association with cryptocurrencies, holds profound potential that beats the digital currencies. Its inherent attributes of decentralization, immutability, and transparency offer a robust framework for secure data storage and transaction management within the AA system. By facilitating a tamper-proof and transparent ledger, blockchain ensures the integrity of financial data and fosters trust among participants, which is major factor in the financial domain. Homomorphic Encryption serves as a powerful tool that maintains data privacy and utility, allowing computations on encrypted data without revealing sensitive information. This encryption paradigm not only strengthens data security but also aligns with stringent global data protection regulations, thereby reinforcing the privacy-protecting credentials of the AA system. The capacity to perform secure computations on encrypted datasets without the need to decrypt ensures that the privacy of individual and institutional financial information is preserved, even amidst complex data analytics and processing. The AA system, a revolutionary model introduced in India, should be made to harness these advanced technologies to resolve the enduring challenges of data security, consent management, and financial inclusion. The system empowers individuals by providing them with unprecedented control over their financial data, simplifying access to financial services, and promoting a transparent and consumer-centric financial environment.

In conclusion, the amalgamation of Blockchain and Homomorphic Encryption within the AA system is a visionary step by India, aligning with its digital India aspirations. It underscores an approach towards redefining financial data sharing, lending, and broader financial services. The AA system, bolded by the budget of 2024, is seen to emerge as a global benchmark for secure, efficient, and inclusive financial data management, heralding a new era of trust, transparency, and empowerment in the digital age.

References

[1] https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1753713

[2] https://finbox.in/blog/what-is-account-aggregator-framework/

[3] https://internationalbanker.com/banking/how-the-account-aggregator-framework-in-india-promises-to-herald-a-new-chapter-in-open-banking-innovation/

[4] https://www.investindia.gov.in/team-india-blogs/account-aggregator-indias-next-digital-innovation

[5] https://sahamati.org.in/what-is-account-aggregator/

[6] https://www.bizadvisors.io/learning/account-aggregator-system-in-india/

[7] https://www.investopedia.com/terms/a/account-aggregation.asp

[8] https://www.pwc.in/industries/financial-services/fintech/fintech-insights/account-aggregators-putting-the-customer-in-charge.html

[9] https://nsdl.co.in/value/Financial_Information_Provider.php

[10] I. Eyal and E. G. Sirer, “Majority is not enough: Bitcoin mining is vulnerable,” in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp. 436– 454.

[11] A. Biryukov, D. Khovratovich, and I. Pustogarov, “Deanonymisation of clients in bitcoin p2p network,” in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 2014, pp. 15–29.

[12] F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 2084–2123, 2016.

[13] NRI, “Survey on blockchain technologies and related services,” Tech. Rep., 2015. [Online]. Available: http://www.meti.go.jp/english/press/2016/pdf/053101f.pdf

[14] D. Lee Kuo Chuen, Ed., Handbook of Digital Currency, 1st ed. Elsevier, 2015. [Online]. Available: http://EconPapers.repec.org/RePEc:eee:monogr:9780128021170

[15] V. Buterin, “A next-generation smart contract and decentralized application platform,” white paper, 2014.

[16] D. Johnson, A. Menezes, and S. Vanstone, “The elliptic curve digital signature algorithm (ecdsa),” International Journal of Information Security, vol. 1, no. 1, pp. 36–63, 2001.

[17] V. Buterin, “On public and private blockchains,” 2015. [Online]. Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[18] “Hyperledger project,” 2015. [Online]. Available: https://www.hyperledger.org/

[19] “Consortium chain development.” [Online]. Available: https://github.com/ethereum/wiki/wiki/Consortium-Chain-Development

[20] L. Lamport, R. Shostak, and M. Pease, “The byzantine generals problem,” ACM Transactions on Programming Languages and Systems (TOPLAS), vol. 4, no. 3, pp. 382–401, 1982.

[21] S. King and S. Nadal, “Ppcoin: Peer-to-peer crypto-currency with proof of-stake,” Self-Published Paper, August, vol. 19, 2012.

[22] “Bitshares - your share in the decentralized exchange.” [Online]. Available: https://bitshares.org/

[23] D. Schwartz, N. Youngs, and A. Britto, “The ripple protocol consensus algorithm,” Ripple Labs Inc White Paper, vol. 5, 2014.

[24] J. Kwon, “Tendermint: Consensus without mining,” http://tendermint.com/docs/tendermint{}v04.pdf, 2014.

[25] S. King, “Primecoin: Cryptocurrency with prime number proof-of-work,” July 7th, 2013.

[26] P. Vasin, “Blackcoins proof-of-stake protocol v2,” 2014. [Online]. Available:

https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf

[27] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, 2014.

[28] V. Zamfir, "Introducing casper the friendly ghost," Ethereum Blog. https://blog.ethereum.org/2015/08/01/introducing-casperfriendly-ghost, 2015.

[29] C. Miguel and L. Barbara, "Practical byzantine fault tolerance," in Proceedings of the Third Symposium on Operating Systems Design and Implementation, vol. 99, New Orleans, USA, 1999, pp. 173–186.

[30] D. Mazieres, "The stellar consensus protocol: A federated model for internet-level consensus," Stellar Development Foundation, 2015.

[31] "Antshares digital assets for everyone," 2016. [Online]. Available: https://www.antshares.org

[32] M. Vukolic, "The quest for scalable blockchain fabric: Proof-of-work ´ vs. bft replication," in International Workshop on Open Problems in Network Security, Zurich, Switzerland, 2015, pp. 112–125.

[33] C. Decker, J. Seidel, and R. Wattenhofer, "Bitcoin meets strong consistency," in Proceedings of the 17th International Conference on Distributed Computing and Networking (ICDCN). Singapore, Singapore: ACM, 2016, p. 13.

[34] D. Kraft, "Difficulty control for blockchain-based consensus systems," Peer-to-Peer Networking and Applications, vol. 9, no. 2, pp. 397–413, 2016.

[35] Y. Sompolinsky and A. Zohar, "Accelerating bitcoin's transaction processing. fast money grows on trees, not chains." IACR Cryptology ePrint Archive, vol. 2013, no. 881, 2013.

[36] A. Chepurnoy, M. Larangeira, and A. Ojiganov, "A prunable blockchain consensus protocol based on non-interactive proofs of past states retrievability," arXiv preprint arXiv:1603.07926, 2016.

[37] https://www.mylawrd.com/what-is-the-account-aggregator-system/

[38] https://internationalbanker.com/banking/how-the-account-aggregator-framework-in-india-promises-to-herald-a-new-chapter-in-open-banking-innovation/

[39] https://www.investindia.gov.in/team-india-blogs/account-aggregator-indias-next-digital-innovation

[40] Alam, Tausif (2018): "Growth Comes with Glitches: It's Not Easy to Recover Money Lost in UPI Transfer," *ENTRACKR*, 11 March, https://entrackr.com/2018/03/upi-transaction-failure/

[41] Baruah, Ayushman (2019): "Rapid Adoption of Account Aggregators can Make India Leader in Digital Economy: Nandan Nilekani," *Livemint*, 4 December, https://www.livemint.com/companies/news/-rapid-adoption-of-account-aggregators-can-make-india-leader-in-digital-economy-11575468667392.html

[42] Bailey, Rishab, Smriti Parsheera, Faiza Rahman and Renuka Sane (2018): "Disclosures in Privacy Policies: Does "Notice and Consent" Work?" *National Institute of Public Finance and Policy*, https://www.nipfp.org.in/media/medialibrary/2018/12/WP_246.pdf

[43] Bhandari, Vrinda and Renuka Sane (2016): "Towards a Privacy Framework for India in the Age of the Internet," https://macrofinance.nipfp.org.in/PDF/BhandariSane2016_privacy.pdf

[44] Blank, Grant, Gillian Bolsover and Elizabeth Dubois (2014): "A New Privacy Paradox: Young People and Privacy on Social Network Sites," *Global Cyber Security Capacity Centre*, https://www.oxfordmartin.ox.ac.uk/downloads/A%20New%20Privacy%20Paradox%20April%202014.pdf

[45] GoI (2019a): "Section 14(2), The Personal Data Protection Bill, 2019," Government of India.

[46] Privacy by Design Foundation (nd): "About IRMA," https://privacybydesign.foundation/irma-en/

[47] (2019b): "Section 18(1), The Personal Data Protection Bill, 2019," Government of India.

[48] (2019c): "Section 25(1), The Personal Data Protection Bill, 2019," Government of India.

[49] (2019d): "Section 84(1), The Personal Data Protection Bill, 2019," Government of India.

[50] Bailey, Rishab, Vrinda Bhandari, Smriti Parsheera and Faiza Rahman (2018): "Response to the Draft Personal Data Protection Bill, 2018," *The Leap Blog*, 20 October, https://blog.theleapjournal.org/2018/10/response-to-draft-personal-data.html.

[51] S. Solat and M. Potop-Butucaru, "ZeroBlock: Timestamp-Free Prevention of Block-Withholding Attack in Bitcoin," Sorbonne Universites, UPMC University of Paris 6, Technical Report, May 2016. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01310088

[52] "Crypto-currency market capitalizations," 2017. [Online]. Available: https://coinmarketcap.com

[53] "The biggest mining pools." [Online]. Available: https://bitcoinworldwide.com/mining/pools/

[54] N. Szabo, "The idea of smart contracts," 1997.

[55] FCA (2019): "Call for Input: Open Finance," *Financial Conduct Authority*, 17 December, https://www.fca.org.uk/publications/calls-input/call-input-open-finance

[56] Khera, Reetika (2019): *Dissent on Aadhaar: Big Data Meets Big Brother*, Hyderabad: Orient BlackSwan.

[57] Kulkarni, Amol, Sidharth Narayan and Swati Punia (nd): "'Users' Perspectives on Privacy and Data Protection," *CUTS International*, https://cuts-ccier.org/pdf/survey_analysis-dataprivacy.pdf

[58] MeitY (nd): "Electronic Consent Framework Technology Specifications—Version 1.1," *Ministry of Electronics and Information Technology*, http://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf

[59] Matthan, Rahul (2017): "Beyond Consent: A New Paradigm for Data Protection," *The Takshashila Institution*, http://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf

[60] NeSL (2018): "Request for Proposal for Selection of Vendor for Design, Development, Installation, Integration, Configuration, Support and Maintenance of Account Aggregation Software," *National e-Governance Services Limited*, https://www.nesl.co.in/wp-content/uploads/2018/06/NADL_RFP_26062018-update.pdf

[61] Pathak, Kalpana, Neil Borate (2020): "Jio May Diversify into Mutual Funds, Other Financial Products," *LiveMint*, https://www.livemint.com/companies/news/jio-may-diversify-into-mutual-funds-other-financial-products-11577900487760.html

[62] Parsheera, Smriti, Faiza Rahman, Renuka Sane, Amba Kak and Vrinda Bhandari (2018): "Response to the White Paper on a Data Protection Framework for India," https://macrofinance.nipfp.org.in/PDF/BKPRS2018WhitePaperResponse.pdf

[63] Rai, Saritha (2020): "India's About to Hand People Data Americans Can Only Dream of," *Bloomberg*, 13 January, https://www.bloomberg.com/news/articles/2020-01-13/india-s-about-to-hand-people-data-americans-can-only-dream-of

[64] RBI (2016): "Master Direction: Non-Banking Financial Company–Account Aggregator (Reserve Bank) Directions," *Reserve Bank of India*, https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598

[65] ReBIT (2019): "NBFC–Account Aggregator: API Specifications," *Reserve Bank Information Technology Private Limited*, 8 November, https://specifications.rebit.org.in/NBFC-AA%20API%20Specification_Core_Final_08Nov.pdf

[66] Raghavan, Malavika and Anubhtie Singh (2020): "Building Safe Consumer Data Infrastructure in India: Account Aggregators in the Financial Sector," 7 January, https://www.dvara.com/blog/2020/01/07/building-safe-consumer-data-infrastructure-in-india-account-aggregators-in-the-financial-sector-part-2/

[67] *Outlook* (2017): "RBI Asks NBFCs Not to Use Coercion during Loan Recovery," 9 November, https://www.outlookindia.com/newsscroll/rbi-asks-nbfcs-not-to-use-coercion-during-loan-recovery/1185289

[68] Tabarrok, Alex and Tyler Cowen (2007): *Modern Principles of Economics*, New York: Macmillan Learning.

[69] Variyar, Mugdha (2017): "ICICI Bank Resumes UPI Transactions on PhonePe," *Economic Times*, 1 February, https://economictimes.indiatimes.com/small-biz/startups/icici-bank-resumes-upi-transactions-on-phonepe/articleshow/56923051.cms?from=mdr

[70] Whittaker, Zack (nd): "India's Largest Bank SBI Leaked Account Data on Millions of Customers," *TechCrunch*, https://techcrunch.com/2019/01/30/state-bank-india-data-leak/

[71] https://www.businesstoday.in/latest/economy/story/account-aggregator-concept-can-be-the-next-upi-in-india-adhil-shetty-of-bankbazaar-348088-2022-09-24

[72] Analysis: https://www.linkedin.com/pulse/account-aggregators-market-analysis-size-share-v5tgf/?trk=article-ssr-frontend-pulse_more-articles_related-content-card

[73] The Miriam-Webster's Dictionary website, 2012. [Online]. Available: http://www.merriam-webster.com

[74] B. Hayes, "Alice and Bob in Cipherspace" in American Scientist vol. 100, 2012, paper 5, p. 362.

[75] K. Thomas. "Sony Makes it Official: PlayStation Network Hacked" PC Computing, pp. 12, April 2011.

[76] B. Adida. "Encryption is (mostly) not magic," Benlog, December 21, 2011, http://benlog.com/articles/2011/12/21/encryption-is-mostly-not-magic

[77] K. Lauter, M. Naehrig, V. Vaikuntanathan, "Can Homomorphic Encryption be Practical?" in CCS'11, 2011, paper 15, pp. 113 - 124.

[78] D. Smith, M. Eggen, R. St. Andre, Transition to Advanced Mathematics, 7th ed., Boston, MA: Brooks/Cole, 2011.

[79] C. Stuntz. "What is Homomorphic Encryption, and Why Should I Care," Craig Stuntz Weblog, March 18, 2010, http://blogs.teamb.com/craigstuntz/2010/03/18/38566/

[80] D. Wu and J. Haven, "Using Homomorphie Encryption for Large Scale Statistical Analysis," 2012.

[81] T. Simonite, "A Cloud that Can't Leak,". Computing News. August 8, 2011.

[82] C. Gentry, (2009). "A Fully Homomorphic Encryption Scheme," Doctoral Dissertation, Symposium on the Theory of Computing, NY, New York, USA, 2009.

[83] C. Gentry and S. Halevi, "Fully Homomorphic Encryption without Squashing Using Depth-3 Arithmetic Circuits," in IEEE' 11, 2011 pp. 107-116.

[84] C. Gentry, S. Halevi, C. Peikert, N. Smart, "Ring Switching in BGV-Style Homomorphic Encryption" in SCN' 12 vol. 7485, 2012, pp. 19-37.

[85] Encrypting Numerical Values [Picture]. Retrieved November 4. 2012, from: http://www.americanscientist.org/issues/pub/alice-and-bob-in-cipherspace

[86] Homomorphic Concatenation [Picture]. Retrieved November 4, 2012, from: http://blogs.teamb.com/craigstuntz/2010/03/18/38566/

[87] https://www.researchgate.net/figure/An-scenario-of-blockchain-branches-the-longer-branch-would-be-admitted-as-the-main-chain_fig4_331425517

[88] https://shiksha.com/online-courses/articles/digital-signing-in-blockchain/

[89] https://www.researchgate.net/publication/337904696_Concept_of_Blockchain_Technology

[90] https://www.researchgate.net/profile/Sonali-Chandel

[91] https://www.theengineeringprojects.com/2021/06/structure-of-a-block-in-blockchain.html

[92] Han Y, Zhang Y, Vermund SH. Blockchain Technology for Electronic Health Records. *International Journal of Environmental Research and Public Health*. 2022; 19(23):15577.