R.M.K GROUP OF ENGINEERING INSTITUTIONS

R.M.K
GROUP OF
INSTITUTIONS

R.M.K
GROUP OF INSTITUTIONS

R.M.K.C.E.T

R.M.K
GROUP OF
INSTITUTIONS

R.M.K
GROUP OF
INSTITUTIONS

Please read this disclaimer before proceeding:

This document is confidential and intended solely for the educational purpose of RMK Group of Educational Institutions. If you have received this document through email in error, please notify the system manager. This document contains proprietary information and is intended only to the respective group / learning community as intended. If you are not the addressee you should not disseminate, distribute or copy through e-mail. Please notify the sender immediately by e-mail if you have received this document by mistake and delete this document from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

22AI001

AI in Blockchain

Batch/Year: 2022-2026/IV

Created by:

**Mr. K. Rajesh Kumar Assist Prof/CSE (CS)
RMKCET**

Date 30.09.2025

Table of Contents

Sl. No.	Topics
1.	Contents
2.	Course Objectives
3.	Pre Requisites (Course Name with Code)
4.	Syllabus (With Subject Code, Name, LTPC details)
5.	Course Outcomes (6)
6.	CO-PO/PSO Mapping
7.	Lecture Plan (S.No., Topic, No. of Periods, Proposed date, Actual Lecture Date, pertaining CO, Taxonomy level, Mode of Delivery)
8.	Activity based learning
9.	Lecture Notes (with Links to Videos, e-book reference, PPTs, Quiz and any other learning materials)
10.	Assignments (For higher level learning and Evaluation - Examples: Case study, Comprehensive design, etc.,)
11.	Part A Q & A (with K level and CO)
12.	Part B Qs (with K level and CO)
13.	Supportive online Certification courses (NPTEL, Swayam, Coursera, Udemy, etc.,)
14.	Real time Applications in day to day life and to Industry
15.	Contents beyond the Syllabus (COE related Value added courses)
16.	Assessment Schedule (Proposed Date & Actual Date)
17.	Prescribed Text Books & Reference Books
18.	Mini Project

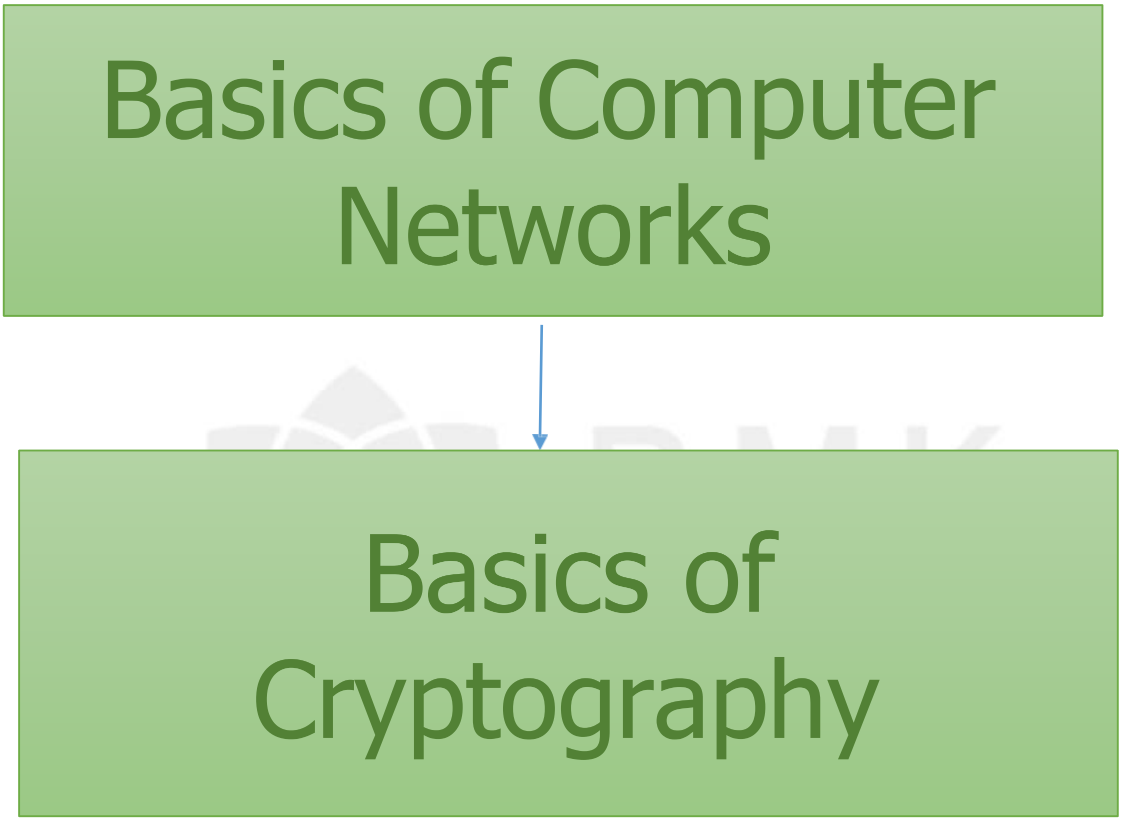
Course Objectives

Course Objectives

- To acquire knowledge in Blockchain Technologies.
- To Understand how block chain and AI can be used to innovate.
- To explain Cryptocurrencies and AI.
- To develop applications using blockchain.
- To understand the limitations and future scope of AI in Blockchain.

PRE REQUISITES

Prerequisites

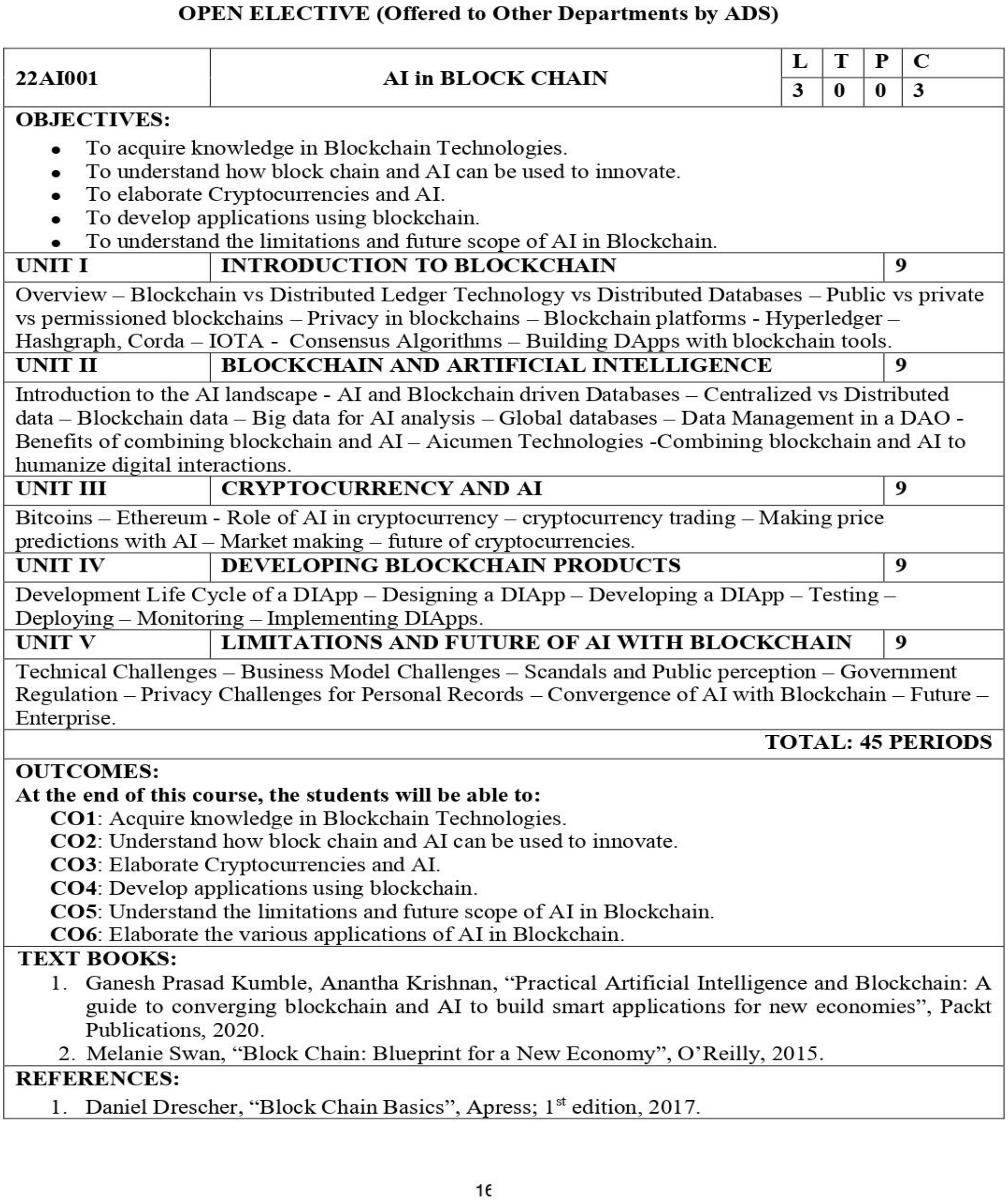


Basics of Computer Networks

Basics of Cryptography

Syllabus

SYLLABUS



OPEN ELECTIVE (Offered to Other Departments by ADS)

22AI001	AI in BLOCK CHAIN	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To acquire knowledge in Blockchain Technologies.
- To understand how block chain and AI can be used to innovate.
- To elaborate Cryptocurrencies and AI.
- To develop applications using blockchain.
- To understand the limitations and future scope of AI in Blockchain.

UNIT I	INTRODUCTION TO BLOCKCHAIN	9

Overview – Blockchain vs Distributed Ledger Technology vs Distributed Databases – Public vs private vs permissioned blockchains – Privacy in blockchains – Blockchain platforms - Hyperledger – Hashgraph, Corda – IOTA - Consensus Algorithms – Building DApps with blockchain tools.

UNIT II	BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE	9

Introduction to the AI landscape - AI and Blockchain driven Databases – Centralized vs Distributed data – Blockchain data – Big data for AI analysis – Global databases – Data Management in a DAO - Benefits of combining blockchain and AI – Aicumen Technologies -Combining blockchain and AI to humanize digital interactions.

UNIT III	CRYPTOCURRENCY AND AI	9

Bitcoins – Ethereum - Role of AI in cryptocurrency – cryptocurrency trading – Making price predictions with AI – Market making – future of cryptocurrencies.

UNIT IV	DEVELOPING BLOCKCHAIN PRODUCTS	9

Development Life Cycle of a DIApp – Designing a DIApp – Developing a DIApp – Testing – Deploying – Monitoring – Implementing DIApps.

UNIT V	LIMITATIONS AND FUTURE OF AI WITH BLOCKCHAIN	9

Technical Challenges – Business Model Challenges – Scandals and Public perception – Government Regulation – Privacy Challenges for Personal Records – Convergence of AI with Blockchain – Future – Enterprise.

TOTAL: 45 PERIODS

OUTCOMES:

At the end of this course, the students will be able to:

CO1: Acquire knowledge in Blockchain Technologies.
CO2: Understand how block chain and AI can be used to innovate.
CO3: Elaborate Cryptocurrencies and AI.
CO4: Develop applications using blockchain.
CO5: Understand the limitations and future scope of AI in Blockchain.
CO6: Elaborate the various applications of AI in Blockchain.

TEXT BOOKS:

1. Ganesh Prasad Kumble, Anantha Krishnan, “Practical Artificial Intelligence and Blockchain: A guide to converging blockchain and AI to build smart applications for new economies”, Packt Publications, 2020.
2. Melanie Swan, “Block Chain: Blueprint for a New Economy”, O’Reilly, 2015.

REFERENCES:

1. Daniel Drescher, “Block Chain Basics”, Apress; 1st edition, 2017.

Course Outcomes

Course Outcomes

CO#	COs	K Level
CO1	Acquire knowledge in Blockchain Technologies	K1
CO2	Understand how block chain and AI can be used to innovate.	K2
CO3	Explain Cryptocurrencies and AI.	K2
CO4	Develop applications using blockchain.	K4
CO5	Understand the limitations and future scope of AI in Blockchain.	K4
CO6	Elaborate the various applications of AI in Blockchain.	K4

Knowledge Level	Description
K6	Evaluation
K5	Synthesis
K4	Analysis
K3	Application
K2	Comprehension
K1	Knowledge

CO – PO/PSO Mapping

CO – PO /PSO Mapping Matrix

CO #	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PS0 3
CO1	3	3	2	1	1	-	-	-	2	-	-	2	3	2	-
CO2	3	2	2	2	2	-	-	-	2	-	-	2	3	2	-
CO3	3	3	2	2	2	-	-	-	2	-	-	2	3	2	-
CO4	3	2	2	2	2	-	-	-	2	-	-	2	3	3	-
CO5	3	2	2	2	2	-	-	-	2	-	-	2	3	2	-
CO6	2	2	1	1	1	-	-	-	2	-	-	2	3	2	-

Lecture Plan

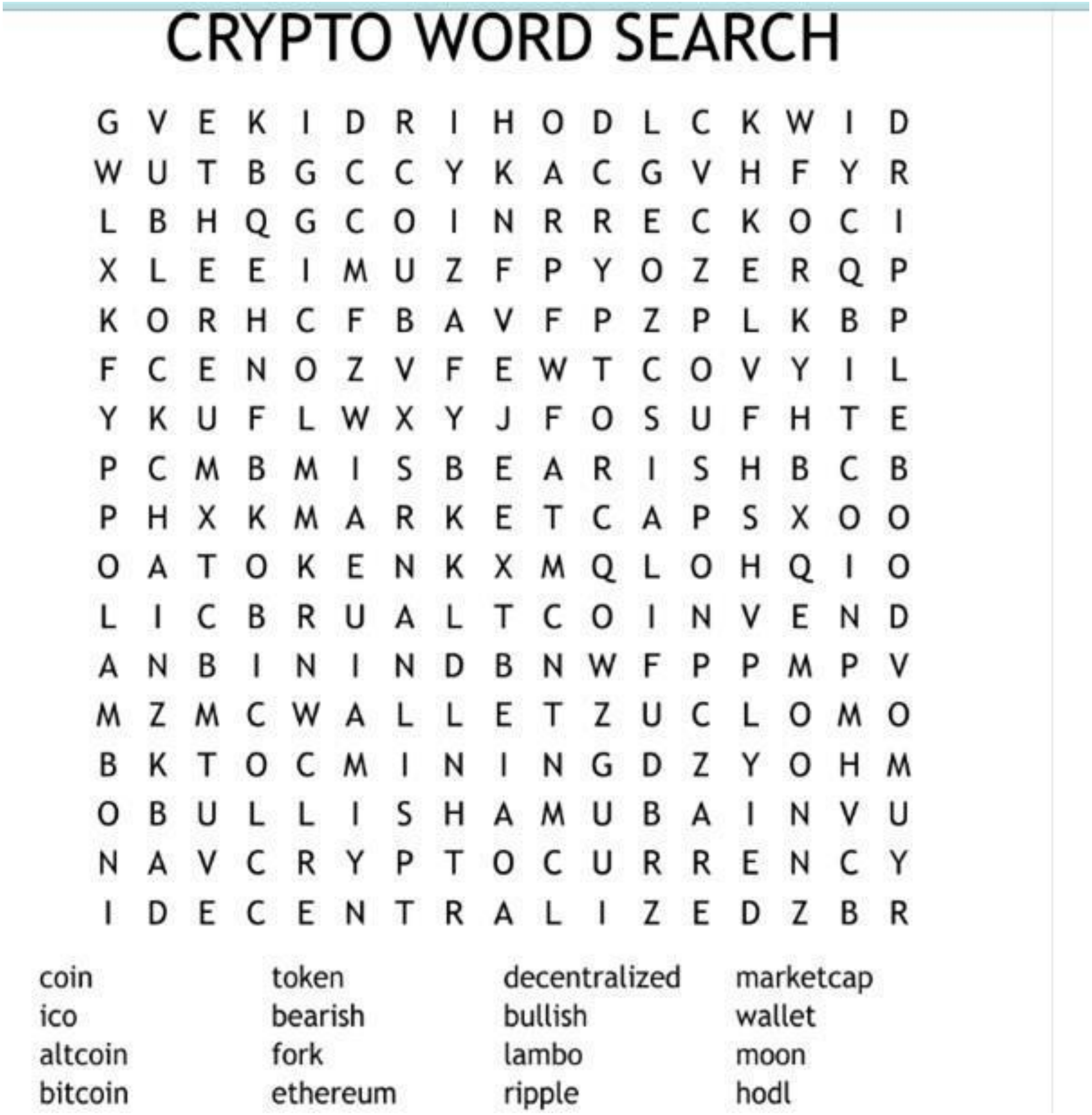
Unit V

Lecture Plan – Unit 5 -Introduction

Sl. No .	Topic	No of Periods	Proposed Date	Actual Lecture Date	CO	Taxo nomy Level	Mode of Deliver y
1	Technical Challenges	1	07.10.2025	07.10.2025	CO5	K2	Chalk & Talk
2	Business Model Challenges	1	08.10.2025	08.10.2025	CO5	K2	Chalk & Talk
3	Scandals and Public perception	1	10.10.2025	10.10.2025	CO5	K2	Chalk & Talk
4	Government Regulation	1	10.10.2025	10.10.2025	CO5	K2	Chalk & Talk
5	Privacy Challenges for Personal Records	1	13.10.2025	13.10.2025	CO5	K3	Chalk & Talk
6	Convergence of AI with Blockchain – Future – Enterprise.	1	5.10.2025	5.10.2025	CO5	K3	Chalk & Talk
7	Convergence of AI with Blockchain – Future – Enterprise.	1	17.10.2025	17.10.2025	CO5	K2	Chalk & Talk
8	Convergence of AI with Blockchain – Future – Enterprise.	1	22.10.2025	22.10.2025	CO5	K3	Chalk & Talk
9	Convergence of AI with Blockchain – Future – Enterprise.	1	24.10.2025	24.10.2025	CO5	K3	Chalk & Talk

Activity Based Learning

Activity Based Learning



CRYPTO WORD SEARCH

G	V	E	K	I	D	R	I	H	O	D	L	C	K	W	I	D
W	U	T	B	G	C	C	Y	K	A	C	G	V	H	F	Y	R
L	B	H	Q	G	C	O	I	N	R	R	E	C	K	O	C	I
X	L	E	E	I	M	U	Z	F	P	Y	O	Z	E	R	Q	P
K	O	R	H	C	F	B	A	V	F	P	Z	P	L	K	B	P
F	C	E	N	O	Z	V	F	E	W	T	C	O	V	Y	I	L
Y	K	U	F	L	W	X	Y	J	F	O	S	U	F	H	T	E
P	C	M	B	M	I	S	B	E	A	R	I	S	H	B	C	B
P	H	X	K	M	A	R	K	E	T	C	A	P	S	X	O	O
O	A	T	O	K	E	N	K	X	M	Q	L	O	H	Q	I	O
L	I	C	B	R	U	A	L	T	C	O	I	N	V	E	N	D
A	N	B	I	N	I	N	D	B	N	W	F	P	P	M	P	V
M	Z	M	C	W	A	L	L	E	T	Z	U	C	L	O	M	O
B	K	T	O	C	M	I	N	I	N	G	D	Z	Y	O	H	M
O	B	U	L	L	I	S	H	A	M	U	B	A	I	N	V	U
N	A	V	C	R	Y	P	T	O	C	U	R	R	E	N	C	Y
I	D	E	C	E	N	T	R	A	L	I	Z	E	D	Z	B	R

coin
ico
altcoin
bitcoin

token
bearish
fork
ethereum

decentralized
bullish
lambo
ripple

marketcap
wallet
moon
hodl

Lecture Notes – Unit 5

Unit V

The blockchain industry is still in the early stages of development, and there are many different kinds of potential limitations. The classes of limitations are both internal and external, and include those related to technical issues with the underlying technology, ongoing industry thefts and scandals, public perception, government regulation, and the mainstream adoption of technology.

Technical Challenges

- A number of technical challenges related to the blockchain, whether a specific one or the model in general, have been identified.
- The issues are in clear sight of developers, with different answers to the challenges posited, and avid discussion and coding of potential solutions.
- Insiders have different degrees of confidence as to whether and how these issues can be overcome to evolve into the next phases of blockchain industry development.
- Some think that the de facto standard will be the Bitcoin blockchain, as it is the incumbent, with the most widely deployed infrastructure and such network effects that it cannot help but be the standardized base. Others are building different new and separate blockchains (like Ethereum) or technology that does not use a blockchain (like Ripple). One central challenge with the underlying Bitcoin technology is scaling up from the current maximum limit of 7 transactions per second (the VISA credit card processing network routinely handles 2,000 transactions per second and can accommodate peak volumes of 10,000 transactions per second), especially if there were to be mainstream adoption of Bitcoin.
- Some of the other issues include increasing the block size, addressing blockchain bloat, countering vulnerability to 51 percent mining attacks, and implementing hard forks

Throughput

- The Bitcoin network has a potential issue with throughput in that it is processing only one transaction per second (tps), with a theoretical current maximum of 7 tps.
- Core developers maintain that this limit can be raised when it becomes necessary.
- One way that Bitcoin could handle higher throughput is if each block were bigger, though right now that leads to other issues with regard to size and blockchain bloat.
- Comparison metrics in other transaction processing networks are VISA (2,000 tps typical; 10,000 tps peak), Twitter (5,000 tps typical; 15,000 tps peak), and advertising networks (>100,000 tps typical).

Latency

- Each Bitcoin transaction block takes 10 minutes to process, meaning that it can take at least 10 minutes for your transaction to be confirmed. For sufficient security, you should wait more time—about an hour—and for larger transfer amounts it needs to be even longer, because it must outweigh the cost of a double-spend attack (in which Bitcoins are double-spent in a separate transaction before the merchant can confirm their reception in what appears to be the intended transac tion).
- Again, as the comparison metric, VISA takes seconds at most. Size and bandwidth The blockchain is 25 GB, and grew by 14 GB in the last year. So it already takes a long time to download (e.g., 1 day). If throughput were to increase by a factor of 2,000 to VISA standards, for example, that would be 1.42 PB/year or 3.9 GB/day. At 150,000 tps, the blockchain would grow by 214 PB/year.
- The Bitcoin community calls the size problem “bloat,” but that assumes that we want a small blockchain; however, to really scale to mainstream use, the blockchain would need to be big, just more efficiently accessed. This motivates centralization, because it takes resources to run the full node, and only about 7,000 servers worldwide do in fact run full Bitcoin nodes, meaning the Bitcoin daemon (the full Bitcoin node running in the

background). It is being discussed whether locations running full nodes should be compensated with rewards.

- Although 25 GB of data is trivial in many areas of the modern “big data” era and data-intensive science with terabytes of data being the standard, this data can be compressed, whereas the blockchain cannot for security and accessibility reasons.
- However, perhaps this is an opportunity to innovate new kinds of compression algorithms that would make the blockchain (at much larger future scales) still usable, and storable, while retaining its integrity and accessibility.
- One innovation to address blockchain bloat and make the data more accessible is APIs, like those from Chain and other vendors, that facilitate automated calls to the full Bitcoin blockchain.
- Some of the operations are to obtain address balances and balances changes, and notify user applications when new transactions or blocks are created on the network. Also, there are web-based block explorers (like https://blockchain.info/), middleware applications allowing partial queries of blockchain data, and frontend customer-facing mobile ewallets with greatly streamlined blockchain data.

Security

- There are some potential security issues with the Bitcoin blockchain. The most worrisome is the possibility of a 51-percent attack, in which one mining entity could grab control of the blockchain and double-spend previously transacted coins into his own account.

- The issue is the centralization tendency in mining where the competition to record new transaction blocks in the blockchain has meant that only a few large mining pools control the majority of the transaction recording.

- At present, the incentive is for them to be good players, and some (like Ghash.io) have stated that they would not take over the network in a 51-percent attack, but the network is insecure.
- Double-spending might also still be possible in other ways—for example, spoofing users to resend transactions, allowing malicious coders to double-spend coins.
- Another security issue is that the current cryptography standard that Bitcoin uses, Elliptic Curve Cryptography, might be crackable as early as 2015; however, financial cryptography experts have proposed potential upgrades to address this weakness.
- Wasted resources Mining draws an enormous amount of energy, all of it wasted.
- The earlier estimate cited was $15 million per day, and other estimates are higher.
- On one hand, it is the very wastefulness of mining that makes it trustable—that rational agents compete in an otherwise useless proof-of-work effort in hopes of the possibility of reward—but on the other hand, these spent resources have no benefit other than mining.
- Usability The API for working with Bitcoind (the full node of all code) is far less user-friendly than the current standards of other easy-to-use modern APIs, such as widely used REST APIs.
- Versioning, hard forks, multiple chains Some other technical issues have to do with the infrastructure. One issue is the proliferation of blockchains, and that with so many different blockchains in existence, it could be easy to deploy the resources to launch a 51-percent attack on smaller chains.
- Another issue is that when chains are split for administrative or versioning purposes, there is no easy way to merge or cross-transact on forked chains.
- Another significant technical challenge and requirement is that a full ecosystem of plug-and-play solutions be developed to provide the entire value chain of service delivery.

- For example, linked to the blockchain there needs to be secure decentralized storage (MaidSafe, Storj), messaging, transport, communications protocols, namespace and address management, network administration, and archival.
- Ideally, the blockchain industry would develop similarly to the cloud-computing model, for which standard infrastructure components—like cloud servers and transport systems—were defined and implemented very quickly at the beginning to allow the industry to focus on the higher level of developing value-added services instead of the core infrastructure.
- This is particularly important in the blockchain economy due to the sensitive and complicated cryptographic engineering aspects of decentralized networks.
- The industry is sorting out exactly how much computer network security, cryptography, and mathematics expertise the average blockchain startup should have—ideally not much if they can rely on a secure infrastructure stack on which this functionality already exists.
- Some of the partial proposed solutions to the technical issues discussed here are as follows:
- Offline wallets to store the majority of coins. Different manner of offline wallets could be used to store the bulk of consumer cryptocoins—for example, paper wallets, cold storage, and bit cards. Dark pools There could be a more granular value chain such that big crypto-exchanges operate their own internal databases of transactions, and then periodically synchronize a summary of the transactions with the blockchain—an idea borrowed from the bank- ing industry.
- Alternative hashing algorithms Litecoin and other cryptocurrencies use scrypt, which is at least slightly faster than Bitcoin, and other hashing algorithms could be innovated.
- Alternatives to proof of work for Byzantine consensus There are many other consensus models proposed—such as proof of stake, hybrids, and

variants—that have lower latency, require less computational power, waste fewer resources, and improve security for smaller chains. Consensus without mining is another area being explored, such as in Tendermint's modified version of DLS (the solution to the Byzantine Generals' Problem by Dwork, Lynch, and Stockmeyer), with bonded coins belonging to byzantine participants.

- Another idea for consensus without mining or proof of work is through a consensus algorithm such as Hyper- ledger's, which is based on the Practical Byzantine Fault Tolerance algorithm.
- Only focus on the most recent or unspent outputs Many blockchain operations could be based on surface calculations of the most recent or unspent outputs, similar to how credit card transactions operate.
- "Thin wallets" operate this way, as opposed to querying a full Bitcoind node, and this is how Bitcoin ewallets work on cellular telephones.
- A related proposal is Cryptonite, which has a "mini-blockchain" abbreviated data scheme.
- To coordinate transactions between blockchains, there are several side chains projects proposed, such as those by Blockstream

Posting bond deposits

- The security of proposed alternative consensus mechanisms like Tendermints's DLS protocol (which requires no proof-of-work mining) could be reinforced with structural elements such as requiring miners to post bond deposits to blockchains.
- This could help resolve the security issue of the "nothing at stake in short time ranges" problem, where malicious players (before having a stake) could potentially fork the blockchain and steal cryptocurrency in a double-spend attack.
- Bond deposits could be posted to blockchains like Tendermint does, making it costly to fork and possibly improving operability and security.

REST APIs

Essentially secure calls in real time, these could be used in specific cases to help usa- bility. Many blockchain companies provide alternative wallet interfaces that have this kind of functionality, such as Blockchain.info's numerous wallet APIs.

Business Model Challenges

Another noted challenge, both functional and technical, is related to business models.

Education and mainstream user-friendly tools are obvious low-hanging fruit (for example, being targeted by Coinbase, Circle Internet Financial, and Xapo), as is improving the efficiency of the entire worldwide existing banking and finance infrastructure like Ripple—another almost "no brainer" project, when blockchain principles are understood. Looking ahead, reconfiguring all of business and commerce with smart contracts in the Bitcoin 2.0 era could likely be complicated and difficult to implement, with many opportunities for service provid- ers to offer implementation services, customer education, standard setting, and other value-added facilitations.

Some of the many types of business models that have developed with enterprise software and cloud computing might be applicable, too, for the Bitcoin economy—for example, the Red Hat model (fee-based services to implement open source software), and SaaS, providing Software as a Service, including with customization. One possible job of the future could be smart contract auditor, to confirm that AI smart contracts running on the blockchain are indeed doing as instructed, and determining and measuring how the smart contracts have self-rewritten to maximize the issuing agent's utility. Scandals and Public Perception One of the biggest barriers to further Bitcoin adoption is its public perception as a venue for (and possible abettor of) the dark net's money-laundering, drug-related, and other illicit activity—for example, illegal goods online marketplaces such as Silk Road. Bitcoin and the blockchain are themselves neutral, as any technology, and are "dual use"; that is, they can be used for good or evil. Although there are possibilities for malicious use of the blockchain, the potential benefits greatly outweigh the potential downsides. Over time, public perception can change as more individuals them- selves have ewallets and begin to use Bitcoin. Still, it must be acknowledged that Bitcoin as a pseudonymous enabler can be used to facilitate illegal and malicious activities, and this invites in-kind "Red Queen" responses appropriate to the blockchain.

Computer virus detection software arose in response to computer viruses; and so far some features of the same constitu- tive technologies of Bitcoin (like Tor, a free and open software network) have been deployed back into detecting malicious players.

Another significant barrier to Bitcoin adoption is the ongoing theft, scandals, and scams (like so-called new altcoin "pump and dump" scams that try to bid up new alt- coins to quickly profit) in the industry.

The collapse of the largest Bitcoin exchange at the time, Tokyo-based MtGox, in March 2014 came to wide public attention. An explanation is still needed for the confusing irony that somehow in the blockchain, the world's most public transparent ledger, coins can disappear and still remain lost months later.

The company said it had been hacked, and that the fraud was a result of a problem known as a "transaction malleability bug." The bug allowed malicious users to double-spend, transferring Bitcoins into their accounts while making MtGox think the transfer had failed and thus repeat the transactions, in effect transferring the value twice.

Analysts remain unsure if MtGox was an externally perpetrated hack or an internal embezzlement. The issue is that these kinds of thefts persist. For example, recent headlines inform us that the Moolah CEO disappeared with $1.4 mil- lion in Bitcoin (October 2014),187 $2 million of Vericoin was stolen (July 2014),188 and $620,000 was stolen in a Dogecoin mining attack (June 2014).189 Blockchain industry models need to solidify and mature such that there are better safeguards in place to stabilize the industry and allow both insiders and outsiders to distinguish between good and bad players.

Oversight need not come from outside; congruently decentralized vetting, confirmation, and monitoring systems within the ecosystem could be established. An analogy from citizen science is realizing that oversight functions are still important, and reinforce the system by providing checks and balances. In DIYgenomics participant-organized research studies, for example, the oversight function is still fulfilled, but in some cases with a wholly new role relevant to the ecosystem—independent citizen ethicists—as opposed to traditional topdown overseers (in the form of a human-subjects research Institutional Review Board).190 Other self-regulating industries include movies, video games, and comic books. There is the possibility that the entire blockchain industry could just collapse (either due to already prognosticated problems or some other factor as yet unforeseen).

There is nothing to indicate that a collapse would be impossible. The blockchain economy does have a strong presence, as measured by diverse metrics such as coin market capitalizations, investment in the sector, number of startups and people working in the sector, lines of GitHub code committed, and the amount of "newspaper ink" devoted to the sector.

Already the blockchain industry is bigger and better established than the previous run at digital currencies (virtual-world currencies like the Second Life Linden dollar). However, despite the progress to date and lofty ideals of Bitcoin, maybe it is still too early for digital currency;
maybe all of the right safe- guards and structures are not yet in place for digital currencies to go fully main- stream (although Apple Pay, more than any other factor, may pave the way to full mainstream acceptance of digital currencies). Apple Pay could quite possibly be enough for the short term. It will be a long time before Bitcoin has the same userfriendly attributes of Apple Pay, such as latency of confirmation time. Government Regulation How government regulation unfolds could be one of the most significant factors and risks in whether the blockchain industry will flourish into a mature financial services industry. In the United States, there could be federal- and state-level legislation;

deliberations continue into a second comment period regarding a much-discussed New York Bitlicense.

The New York Bitlicense could set the tone for worldwide regulation. On one hand, the Bitcoin industry is concerned about the extremely broad, wide-reaching, and extraterritorial language of the license as currently proposed. The license would encompass anyone doing anything with anyone else's Bitcoins, including basic wallet software (like the QT wallet).192 However, on the other hand, regulated consumer protections for Bitcoin industry participants, like KYC (know your customer) requirements for money service businesses (MSBs), could hasten the mainstream development of the industry and eradicate consumer worry of the hacking raids that seem to plague the industry. The deliberations and early rulings of worldwide governments on Bitcoin raise some interesting questions. One issue is the potential practical impossibility of carrying out taxation with current methods.

A decentralized peer-to-peer sharing economy of Airbnb 2.0 and Uber 2.0 run on local implementations of OpenBazaar with individuals paying with cryptocurrencies renders traditional taxation structures impossible. The usual tracking and chokehold points to trace the consumption of goods and services might be gone. This has implications both for taxation and for the overall measurement of economic performance such as GDP calculations, which could have the beneficial impact of drawing populaces away from being overly and possibly incorrectly focused on consumption as a wellness metric. Instead, there could be an overhaul of the taxation system to a consumption-based tax on large-ticket visible items such as hard assets (cars, houses). Chokehold points would need to be easily visible for taxation, a "tax on sight" concept.

A potential shift from an income tax–based system to a consumption tax–based system could be a significant change for societies. A second issue that blockchain technology raises with regard to government regulation is the value proposition offered by governments and their business model.

Some argue that in the modern era of big data, governments are increasingly unable to keep up with their record-keeping duties of recording and archiving information and making data easily accessible. On this view, governments could become obsolete because they cannot fund themselves the traditional way—by raising taxes.

Blockchain technology could potentially help solve both of these challenges, and could at minimum supplement and help governments do their own jobs better, eventually making classes of government-provided services redundant. Recording all of a society's records on the blockchain could obviate the need for entire classes of public service.

This view starkly paints governments as becoming redundant with the democratization of government features of the blockchain. However, just as there might be both centralized and decentralized models to coordi- nate our activities in the world, there could likely be roles for both traditional government and new forms of blockchain-based government. There might still be a role for traditional centralized governments, but they will need to become economically rationalized, with real value propositions that resonate with constituencies, shrink costs, and demonstrate effectiveness.

There could be hybrid governments in the future, like other industries, where automation is the forcing function, and the best "worker" for the job is a human/algorithmic pairing.193 Perfunctory repetitive tasks are automated with blockchain registries and smart contracts, whereas government employees can move up the value chain.

Privacy Challenges for Personal Records

There are many issues to be resolved before individuals would feel comfortable storing their personal records in a decentralized manner with a pointer and possibly access via the blockchain.

The potential privacy nightmare is that if all your data is online and the secret key is stolen or exposed, you have little recourse. In the current cryptocurrency architecture, there are many scenarios in which this might happen, just as today with personal and corporate passwords being routinely stolen or databases hacked—with broad but shallow consequences; tens of thousands of people deal with a usually minor inconvenience. If a thorough personal record is stolen, the implications could be staggering for an individual: identity theft to the degree that you no longer have your identity at all.

Overall: Decentralization Trends Likely to Persist However, despite all of the potential limitations with the still-nascent blockchain economy, there is virtually no question that Bitcoin is a disruptive force and that its impact will be significant. Even if all of the current infrastructure developed by the blockchain industry were to disappear (or fall out of popularity, as virtual worlds have), much of their legacy could persist. The blockchain economy has provided new larger-scale ideas about how to do things. Even if you don't buy into the future of Bit- coin as a stable, long-term cryptocurrency, or blockchain technology as it is currently conceived and developing, there is a very strong case for decentralized models. Decentralization is an idea whose time has come. The Internet is large enough and liquid enough to accommodate decentralized models in new and more pervasive ways than has been possible previously. Centralized models were a good idea at the time, an innovation and revolution in human coordination hundreds of years ago, but now we have a new cultural technology, the Internet, and techniques such as distributed public blockchain ledgers that could facilitate activity to not only include all seven billion people for the first time, but also allow larger-scale, more complicated coordination, and speed our progress toward becoming a truly advanced society. If not the blockchain industry, there would probably be something else, and in fact there probably will be other complements to the blockchain industry anyway. It is just that the blockchain industry is one of the first identifiable large-scale implementations of decentralization models, conceived and executed at a new and more complex level of human activity.

The convergence of AI and blockchain

Billions of dollars' worth of assets are managed by innovative financial instruments on public blockchain networks such as Ethereum. AI is used in predictive healthcare, cancer research, and contact-tracing COVID-19 infections. Both technologies are serving humans in an indirect manner.

The future of converging AI and blockchain

Several experiments are being undertaken on building new waves of digital solutions where AI and blockchains can co-exist to deliver optimal solutions that enable faster decision making and provide the desired transparency to all stakeholders.

In the following diagram, a general representation of the hybrid solution architecture of a DIApp is provided

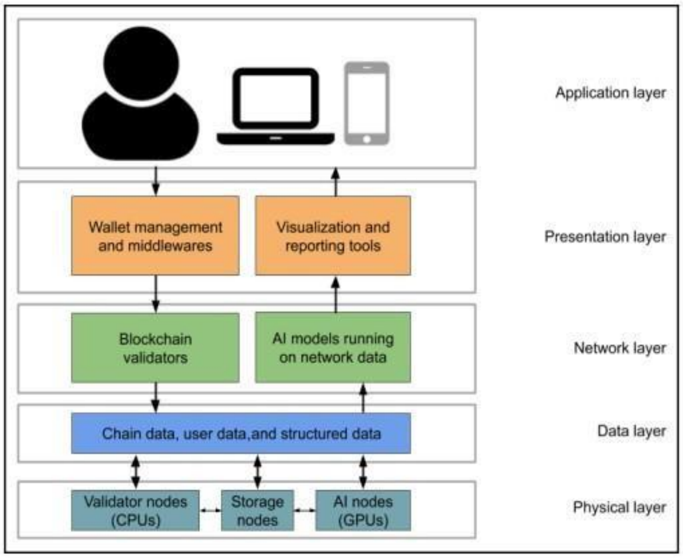


Fig 9.1: Reference solution architecture for a DIApp

Figure Reference solution architecture of DIApps

The preceding diagram is a pictorial representation of reference architecture for the majority of DIApp solutions.

OSI is a network model conceptualized in the late 1970s. It was published by the International Standards Organization (ISO) in 1984. The ISO model is made up of seven layers: Physical, Data link, Network, Transport, Session, Presentation, and Application.

Five layers of the solution architecture from the preceding diagram are as follows:

Application layer:

The application layer consists of end users and client software installed on mobiles, laptops, and devices. Users will sign transactions through the middleware and access data through reporting tools from the presentation layer.

The application layer also represents a wider range of deployment facilities, and administration of the DIApp through special tools such as an Identity and Access Management (IAM) manager.

Presentation layer:

The presentation layer consists of backend functionalities manifested in the clients, which are not visible to end users.

This layer includes all the supporting tools and software required to enable blockchain functionalities in an application such as signing a transaction, propagating a signed transaction, and receiving results.

The layer also contains tools required to enable AI-related functionalities that can help users gain insights from the application, such as visualization and reporting.

Network layer:

As the name suggests, the network layer consists of service networks consisting of blockchain validator nodes running a software bundle designated for verifying user transactions and blocks formed by other nodes in the blockchain network. Similarly, the network layer also consists of several AI services based on machine learning (ML) algorithms and deep learning (DL) algorithms. Some of these AI services may also use artificial neural networks (ANNs), convolutional neural network (CNNs), and so on.

Data layer:

The data layer defines, persists, and provides the interface for applications to access user data, network data, and other processed data.

The data layer is a connecting layer between the network layer and the physical layer.

Applications, validation software, and AI models will access the critical information from this layer through proper authentication methods configured by administrators.

Physical layer:

The physical layer represents all the Graphics Processing Unit (GPU) nodes, virtual machines (VMs), and storage nodes used to store the data and perform complex computations.

This layer also addresses the core management of infrastructure, through a variety of DevOps practices

Converging AI and blockchain in enterprise

The global market size of Enterprise Resource Planning (ERP) software is expected to reach around USD 70 billion over the next 5 years. Over the past few years in the last decade, leading companies in the ERP software market, such as SAP and Oracle, have consistently pushed for the use of cloud and other emerging technologies. Several pilots were also launched in the interest of reducing costs and increasing overall productivity on the floor across various solution spaces, including Customer Relationship Management (CRM) and Supply Chain Management (SCM). There are a few niche use cases that could leverage the best of AI and blockchain technologies, along with other peripheral technologies, such as decentralized data management and Decentralized ID (DID) management.

Let's now explore some of the use cases that could enhance current enterprise software with blockchain and AI technologies.

1. Customer service

When it comes to customer service, it is somehow perceived that companies and brands from developing countries, including India, are not very great at serving their customers. This perception may be true, for the following general reasons: A lack of necessary talent A lack of proper staff training There is also an issue with incentives and endless shifts that could prevent personnel from giving their best. This issue could be resolved by using a combination of blockchain and AI technologies.

As-is scenario

Customer service agencies and call centers are usually plagued by issues including the following:

General lack of context: As a customer and user of a premium phone brand, you may want to visit their service center and get the whole picture on what is going wrong with your mobile phone. However, instead of simply scanning the mobile IMEI and pulling the latest records, the representative might ask you to fill in a form and include all the details pertaining to the current issue you are facing with your phone. This issue can be resolved very easily by bringing context to service desks.

To-be scenario

Using the power of blockchain and AI, service desk personnel should be able to automatically identify and verify the owner of the phone.

If the same could be authenticated successfully with a signature using the private key or through sophisticated Zero-Knowledge Proofs (ZKP), the same personnel should be automatically granted access to the phone log locally to perform basic diagnostics.

The use of decentralized data storage services such as MoiBit (www.MoiBit.io) to store the necessary diagnostic files. These files can be hosted by the mobile owner and used by personnel for further examination of the problem with strict sharing options set by the owner. MoiBit can also be used by the personnel to verify the ownership of the mobile through sale deeds or purchase receipts.

Possible solution

We can use Decentralized Identifiers (DIDs) to identify each mobile owner in the mobile company's retail side of the supply chain management software. Instead of a silo system, this supply chain would be a consortium of phone manufacturers, who could also recognize the owner of this premium phone, meaning that one DID could represent the ownership of one or more mobiles Now, in situations where persistence of documents and files are necessary, we can use MoiBit due to its ease of use and also the granular level of access control you could use to provide privacy to the owner of the mobile (before and after purchasing the phone).

This also means that we can use MoiBit to store the logs of the owner's phone securely in their own dedicated infrastructure or a common network without paving the way for centralization or illicit data mining activities.

Once the phone is able to log all the data, we just need to apply predictive maintenance machine learning algorithms to ensure that customer service is available even before the user identifies the need for help.

The following diagram summarizes our approach in a compartmentalized reference structure to help you understand the solution better

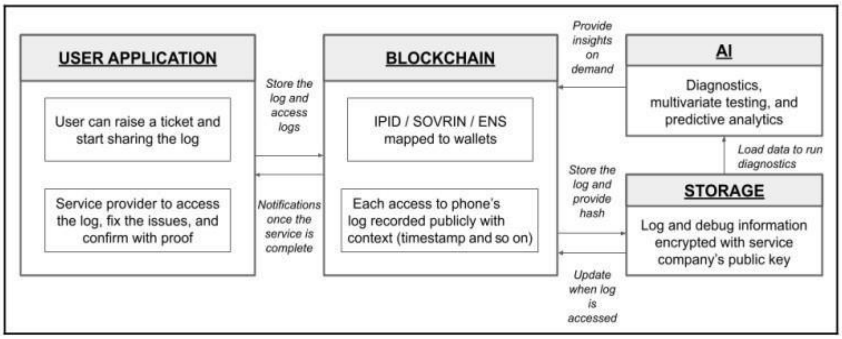

USER APPLICATION
User can raise a ticket and start sharing the log
Service provider to access the log, fix the issues, and confirm with proof
Store the log and access logs
Notifications once the service is complete
BLOCKCHAIN
IPID / SOVRIN / ENS mapped to wallets
Each access to phone's log recorded publicly with context (timestamp and so on)
Provide insights on demand
Store the log and provide hash
Update when log is accessed
AI
Diagnostics, multivariate testing, and predictive analytics
Load data to run diagnostics
STORAGE
Log and debug information encrypted with service company's public key

Fig 9.2: Reference solution architecture for addressing customer service issues

As shown in the preceding reference solution architecture diagram, the suggested solution is split across four components,

User application: There could be one application that enables users to raise tickets for an issue. The app can also request users to allow access to the logs in order to provide a secure backup, and access to the log on MoiBit's decentralized storage. On the other hand, we could have another application that can provide the delegation of tickets to a service executive. The service executive can be notified of the new ticket assigned to them

Blockchain:

The user application should allow customers to share more details about the problem they are facing. The details relating to the problem may include product information and technical specifications.

If the problem persists, the user should be able to share the boot log or any other sensitive information.

To enforce transparency in audit and bring accountability to the access given to such sensitive data, we require all verified personnel to perform service-related operations through a specific wallet address.

These wallet addresses can be further enhanced with the help of DIDs and name services such as the Ethereum Name Service (ENS). The blockchain network will not only provide wallets for customers and service personnel, but also record each read and write operation, meaning that every update (write) made to the log will be recorded with a new hash embedded in a transaction. Similarly, every time a member of the service personnel accesses the user's log, a transaction is emitted along with a notification. Once the service ticket is resolved, the service personnel will provide suitable evidence and stake a resource in order to claim and verify that the service job is closed. If a majority in the network is unable to verify the claim with the given proofs, the stake can be diluted, causing an economic loss to the personnel who are acting dishonestly.

Storage: We require a decentralized storage service that can securely log personal information and other proofs in order to support the aforementioned logic. We can use MoiBit to store the information, encrypting it only between the user and the service personnel. Service personnel can now use their designated wallet in order to access the logs, perform analysis, and provide suitable support. The specifics regarding analysis will be covered by the following component.

AI:

Now that the information is safely stored on MoiBit, we can build a simple model that can run basic diagnostics followed by multivariate testing on the data. The data can be made accessible by using the MoiBit API along with the service professional's credentials already registered on the ticketing contract in the blockchain. The API will not provide unwarranted access to data by service personnel or other users who are not assigned the ticket. This idea could be applied across many products that require active maintenance, without harming user privacy or the company's IP.

Hence, the scope can be expanded to automobiles, shop floor machines, 3D printers, mission-critical systems in the military as well as other consumer electronics, such as refrigerators, air conditioners, and security cameras

2. Performance management

Enterprise companies require undivided attention from the board and its executives in managing various performance factors.

These factors drive revenue and profits and they are communicated through Key Performance Indicators (KPIs), which are used to identify any potential growth or pitfall in the business.

As the company progresses toward achieving a number of business objectives, it is important to understand the potential issues coming their way.

These issues could slow down the momentum needed to achieve the business objective or, in worst case scenarios, end up sabotaging the objective altogether.

As-is scenario

Over the past few years in the previous decade, a considerable amount of Research and Development (R&D) has been undertaken in analyzing KPIs, enabling boardrooms to make effective decisions in less time.

However, the quality of the data used to transform business models, or to optimize them, could be revisited.

Every business process that is digitized today has both pros and cons. The pros are quite obvious in terms of automation, along with the reduced time and effort required to achieve an objective.

However, the cons are a lack of transparency, among a wider range of issues associated with internal compliance with the process. There could be hidden blind spots in a digitized business process that may not be effective in churning out the critical data required over the longer term.

Let's take food delivery apps for example. There are multiple applications giving users the option to order food remotely and have it delivered in 30 minutes or less. The process of ordering the food from a user's app, to reaching the kitchen of a restaurant, to delivering the cooked food from the restaurant to the user's address, is already a digital process today.

Many of these food delivery app companies would have established KPIs such as the Number of cancelled orders, the Number of delayed deliveries, and the Number of orders placed. These KPIs are internally dependent on the outcome of the process, and AI is already being used in monitoring such KPIs through big data analytics.

A number of issues looming around limited data being gathered to analyze the business include the following:

Lack of incentivization: There are a few issues associated with plugging into data from the metrics alone. Consumer-facing apps will only sustain if they actively listen to the user.

Let's all ask the question of how many times have we honestly rated a food delivery experience in the app? And even if we did take the time to provide valuable feedback, how many times were we incentivized by the app to do so? Most of us might answer here with a no, at least to the latter question. Hence, there is a need to gamify this digital process to harness the real information from the end user and optimize the process for better outcomes.

To-be scenario

There is always a hunger in a consumer-facing company to grow and offer better customer service. In the future, apps should consider rewarding customers by paying them in cryptocurrency for each successful review submission. This will help incentivize users to provide genuine feedback for each service instance rendered by the app.

In this process of collecting user reviews, companies would also be able to solve some of the current inefficiencies and cut the costs associated with a particular type of service and make business decisions.

Possible solution

You could consider building a novel food delivery app that not only handles normal operations, but identifies each user with a decentralized identifier DID. This is step 1 on the road to user privacy. With the DID, you could associate a wallet that is used to remit a digital currency for every successful review. You could also consider applying form validation and rate limiting techniques to ensure that bad actors are not gaming this system just to collect the rewards. If the rules of the app consider the review content compelling enough, a bot can be used to quickly remit the digital currency and also start a dialogue with the user, notifying them that the feedback is greatly appreciated

Later on, the bot can also be used to communicate, if the user wishes, to brief a little more on the problem. This is called an interactive feedback system. Any extended information received by users via chatbot can later be tokenized and sent to models using narrative analysis and content analysis.

Using this approach, the new enhanced versions of the app are poised to receive more feedback, elevate the quality of service, and also cut down costs as regards unnecessary components in the service. The following diagram summarizes our approach in a compartmentalized reference structure to help you understand the solution better

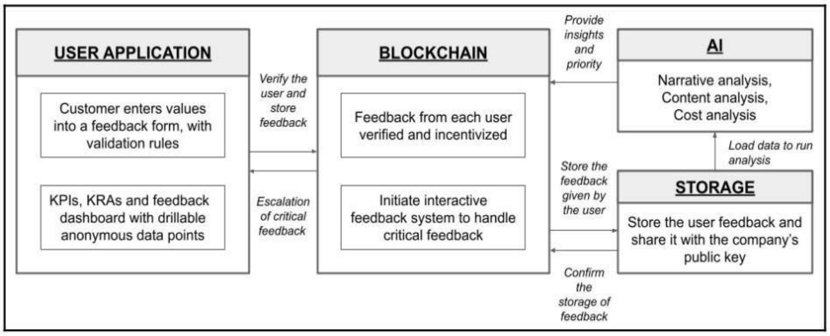

USER APPLICATION
Customer enters values into a feedback form, with validation rules
KPIs, KRAs and feedback dashboard with drillable anonymous data points
Verify the user and store feedback
Escalation of critical feedback
BLOCKCHAIN
Feedback from each user verified and incentivized
Initiate interactive feedback system to handle critical feedback
Provide insights and priority
Store the feedback given by the user
Confirm the storage of feedback
AI
Narrative analysis, Content analysis, Cost analysis
Load data to run analysis
STORAGE
Store the user feedback and share it with the company's public key

Fig 9.3: Reference solution architecture for gamifying the user feedback system in order to increase the performance of a product or service

As shown in the preceding reference solution architecture diagram, the suggested solution is split across four components, namely:

User application: There could be one application or page within an existing application to facilitate a user feedback system. This system will ask users to provide valuable feedback on the product or service availed by the user, in exchange for a cryptocurrency. This is a new method of incentivizing a user with a liquid asset, compared to loyalty points that may come with strings attached. There could also be a need to develop a separate dashboard for companies and vested stakeholders of the product or service, who need to be given the topline information on the feedback. Apart from providing the topline information such as the KPIs and KRAs, the dashboard also needs to provide an interface to drill down on the feedback in order to better understand the context.

Blockchain: In order to gamify the feedback process with cryptocurrencies and limit the bad actors and Sybil attacks, we need to use a blockchain network. The blockchain network will be used to designate a wallet for each user of the product or service who opts in to provide feedback. When the feedback is validated at the client level, the data needs to be signed by the user's designated wallet in order to verify and confirm their action. When the wallet is used to sign the data, the resulting transaction is then sent to the blockchain network. The network validates and executes an oracle or a webhook in order to store the feedback data in a secondary network.

Storage: We need a decentralized storage service that enables users to store their feedback data in a permissive manner. In most of the feedback systems we use today, the user loses control over the feedback data once it leaves the app. This needs to change in order to provide more control to the user. We can use any IPFS-based network, such as MoiBit, to persist the feedback in a permissive manner. The feedback data will be encrypted to the user and the company rendering said product or service. This data can now be used by companies in a permissive manner to assess, evaluate, and enhance their service to customers.

AI:

Once the feedback data is stored safely in MoiBit, and shared with the respective companies, you can build an AI model that uses the MoiBit API to fetch the data remotely with appropriate authentication. Once the data is loaded, we can use several NLP techniques, such as content and context analysis, in order to gain a preliminary understanding without any human effort. Once a priority is set by the model, we could use chatbots to initiate a resolution to the feedback. While the conversation is progressing, we can also use narrative analysis in order to gain a richer context of the situation. If the resolution is not achieved by a well-trained chatbot, we can provide the result of the entire analysis to a human representative in order to identify and rectify any gaps. The human representative will resolve the feedback by making a final decision based on the supporting data made available by the AI models.

Data security

Securing trade secrets, critical market data, and other sensitive information of a growing enterprise is of high importance in order to preserve the company's strategic and tactical position among its competitors. Although there were several items of special security software offered to enterprises in the previous generation, only a handful were able to protect the information from a new wave of attacks leveraging cutting-edge techniques.

The next wave of information or data security software could be powered by blockchain and AI in order to empower enterprises and reduce potential attacks as far as possible.

As-is scenario

The traditional model of enterprise data management moved from on-premises Knowledge Management Systems (KMSs) to data warehouses. Later on, we saw more innovation happening on the cloud, wherein companies were encouraged to move from on-site infrastructure to a hybrid model of storing all the information remotely in servers managed by Cloud Service Providers (CSP) such as Azure and Amazon Web Services. Further to the adoption of the cloud, a more practical approach was proposed, wherein relevant pieces of data could either be stored on the cloud or on-premises (on-prem) to provide flexibility.

Although the cloud is gaining traction in terms of usage, a significant share of the market is yet to take the brave step toward a complete cloud migration. Concerns such as control and ownership of data could be a source of worry to some decision makers and thereby be inhibiting this movement.

The top issue faced in managing data security on the public cloud is as follows:

Granular access control and encryption:

Enterprise applications mostly handle critical information about the company's financial data, trade secrets, design files, and leads on a potential client. Due to the nature of the information being used and circulated, there is a need to be extra vigilant regarding the sharing of knowledge. In the wrong hands, leaked information about the company can result in devastating effects on the company's performance.

To-be scenario

Although blockchain technology alone may not be a key enabler for enterprises, it offers companies exposure to a decentralized infrastructure. In this decentralized infrastructure, companies can share, trade, and exchange resources to form a stronger business network. This new method of sharing infrastructure based on blockchains can be less prone to cyber attacks and certainly immune from data corruption intended by malicious users. We will move from a competitive mode to a collaborative mode wherein non-critical resources could be pooled by all the stakeholders in order to achieve a common business goal.

In the future, enterprise applications should be able to leverage blockchain for full accountability and a transparent view of access to corporate information. These applications could also be equipped with Business Intelligence (BI) tools and AI services, to offer insights based on access patterns in order to neutralize any cyber threat.

Possible solution

Decentralized databases and data services such as MoiBit to build a document-centric application that can be designed effectively may be considered to ensure that the data integrity of the business documents will stay intact. We can also use a blockchain separately to store the metadata of the files and maintain access logs. In conjunction with using blockchains, you may also build new visualization tools and basic regression models that allow users to draw insights from the data stored in said decentralized database. User authentication can be enhanced dramatically with the advent of several DIDs and name resolvers.

The following diagram summarizes our approach in a compartmentalized reference structure to help you understand the solution better:

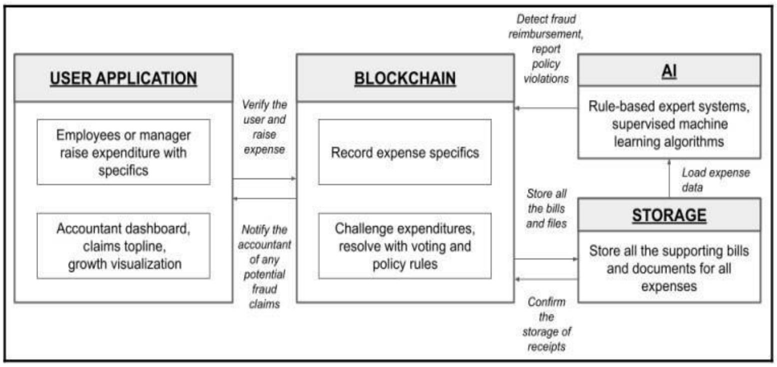

USER APPLICATION
Employees or manager raise expenditure with specifics
Accountant dashboard, claims topline, growth visualization
Verify the user and raise expense
Notify the accountant of any potential fraud claims
BLOCKCHAIN
Record expense specifics
Challenge expenditures, resolve with voting and policy rules
Detect fraud reimbursement, report policy violations
AI
Rule-based expert systems, supervised machine learning algorithms
Load expense data
Store all the bills and files
STORAGE
Store all the supporting bills and documents for all expenses
Confirm the storage of receipts

Fig 9.4: Reference solution architecture for identifying security threats in ERP systems with the help of blockchain and AI

Reference solution architecture for identifying security threats in ERP systems with the help of blockchain and AI

As shown in the preceding reference solution architecture diagram, the suggested solution is split across four components, firstly:

User application:

As usual, the application component will comprise the client applications used by employees and admins. The employee application could be a simple Customer Relationship Management (CRM) application that stores the lead data securely on an IPFS-based permissive network such as MoiBit. In the CRM application, we could have a basic feature that allows employees to create a new lead based on the information gathered by the sales employee. The application could rely on custom name resolvers in order to verify employees. On the other hand, we also need an administrator dashboard in order to closely monitor the health of the network, followed by a list of recent accesses made by employees. Based on the visualization provided by the visualization tools, the admin can take the actions necessary to ensure the stability of the network. An administrator dashboard could also have a multisig-based capability, thereby ensuring that the power to make changes is not vested in a single person.

The overall security of the system can be enhanced by at least three degrees as follows:

1-step verification: Company email ID and password.

2-step verification: OTP from the employee's cell phone and/or authenticator.

3-step verification: Verify ownership of a wallet belonging to a particular name service. For example, you can ensure that the application allows access only if you have a wallet address that can be resolved to companyxyz.eth. Company XYZ's employee, Ms. ABC, will be provided with a wallet address resolved by the name abc.companyxyz.eth. If the user is unable to prove that they own a wallet resolved by abc.companyxyz.eth, the app should not grant access.

It should be mentioned that the aforementioned enhancements could work as an enhancement alongside enterprise authentication mechanisms including Fast Identity Online (FIDO) keys.

Blockchain:

The blockchain network will resolve the name service in order to confirm ownership of the wallet. Once the wallet is authorized, the blockchain network is also responsible for facilitating the storage of information in a secondary network. Once the storage operation is complete, the smart contracts in the blockchains will emit transactions for every successful or failed access to a document. This access data is primarily stored on the blockchain and later copied to the secondary storage network for further analysis into failed access to resources

Storage:

We need a decentralized storage service that can cache all the access logs so that AI systems can get faster access to the data without creating a bottleneck in the primary blockchain network. By using an IPFS-based network, we preserve the immutability features of the blockchain, and also retain the ability to verify the cached content.

AI:

Now that the access logs are copied and cached into MoiBit, the administrator can choose a custom trained model of their own or use an unsupervised machine learning technique to detect anomalies in terms of access to a number of critical documents. Once a pattern is generated and analyzed, the anomalies can be recognized in order to act on the attacks.

3. Finance management

Most enterprise companies survive based on the stable revenue generated by established product lines. Depending on the products or services, these companies may be generating income ranging from millions to billions of dollars annually. Such huge volumes of income demand proportional costs in the form of expenses that need to be audited regularly and ensure that the books are intact. It is also important to note that most of the large-scale companies who generate such large revenues are public companies, with many public stakeholders watching the growth of the company's sales closely.

As-is scenario Traditional accounting software used to allow employees such as a clerk or an accountant to manually bill for the sales of goods. However, in today's generation of finance software, accounting modules are already closely knit together with various front-facing modules including Point of Sale (POS), which is used to bill the items and generate invoices. Although a majority of accounting operations are now being shifted from manual entries to bar code-driven automation, there could be a high risk of financial fraud and the fudging of numbers in the books.

The top issue faced by enterprises in finance management is as follows: **Accounting scandals:** An accounting scandal is defined as an intentionally orchestrated process of manipulating the financial statements of a company in order to achieve the purpose of deceiving someone. Most countries consider this a criminal act, as it allows individual employees and the company to overemphasize an asset or misrepresent current financial liabilities, thereby exposing the stakeholders to risk.

To-be scenario

In the future, accounting software will not only be automated with other modules. Transparency may be embraced by using blockchain in order to enable simpler and cheaper audits for interested parties. Also, accounting applications should be able to leverage deep learning techniques to identify any potential anomalies in the company's cash flow transactions.

Possible solution

You can consider building an accounting application that maintains a virtual ledger recording the ledger as per the norms. The accounting application can also transparently broadcast the virtual ledger if the company wishes to do so. Meanwhile, this blockchain application will also be responsible for managing the states of every wallet, so as to monitor any bad actors within a department. The application can also leverage deep learning models to detect anomalies found in the financial statements and to ensure that no fraudulent acts are being committed. The following diagram summarizes our approach in a compartmentalized reference structure to help you understand the solution better:

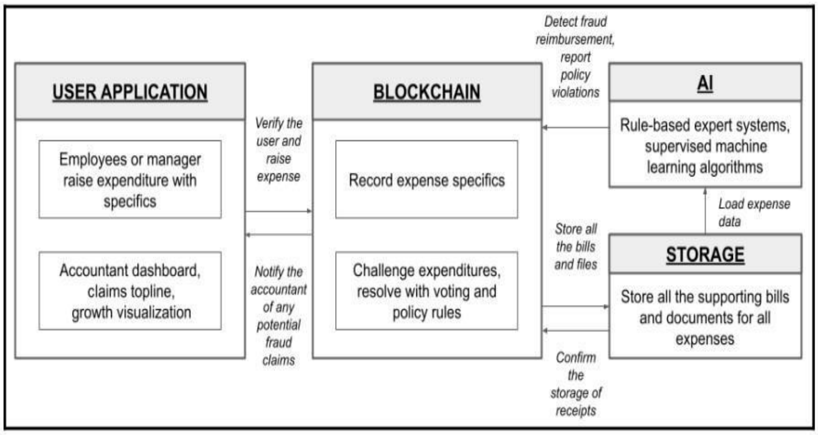

USER APPLICATION
Employees or manager raise expenditure with specifics
Accountant dashboard, claims topline, growth visualization
Verify the user and raise expense
Notify the accountant of any potential fraud claims
BLOCKCHAIN
Record expense specifics
Challenge expenditures, resolve with voting and policy rules
Detect fraud reimbursement, report policy violations
Store all the bills and files
Confirm the storage of receipts
AI
Rule-based expert systems, supervised machine learning algorithms
Load expense data
STORAGE
Store all the supporting bills and documents for all expenses

Fig 9.5: Reference solution architecture for managing expenditures and identifying any fraudulent transactions

Reference solution architecture for managing expenditures and identifying any fraudulent transactions

As shown in the preceding reference solution architecture diagram, the suggested solution is split across four components, namely:

User application:

There may be one form that could be used by employees to claim expenses. You can simply build a secure application as explained in the previous Data security section and allow users to raise the expenses. There may be another form that can be used by the accounts department in order to review and resolve claims. Although you could automate a significant portion of this section today, we can rethink transparency and fraud detection with the help of blockchain and AI, respectively.

Blockchain:

The blockchain network will provide wallets for each employee, including the accounts department, to manage the company's capital. The blockchain-based smart contract can also be used to challenge a few suspected transactions in a democratic manner in order to resolve expenses within a department.

Storage: We need a decentralized storage service that can store the bill copies, receipts, purchase orders, and many other supporting documents provided by the employees who raise the expense claims. These supporting documents will be reviewed by the accountant, alongside an AI model that reduces the human effort involved in tracing the origin and verifying the authenticity of the transactions made by employees. We require an IPFS-based network that can persist these documents without giving way to any cyber attack or posting invoices with doctored values. The supporting documents can be encrypted and shared between the accounts department for further review.

AI: Now that the supporting documents are stored in an IPFS-based network such as the MoiBit, we can use the APIs and the accounts department's credentials in order to load the expense data into machine learning algorithms in order to identify potential fraudulent expenses. Rule-based expert systems can also be used to identify any claims that are beyond the scope of a company's policy so that the claim can be rejected without expending too much energy. Following this detailed walkthrough of problems across several domains in the enterprise landscape, let's now explore the problems faced by governments.

4. Converging AI and blockchain in government

A lot of progress in society depends on services offered by local government, as well as national-level governments. Citizens are dependent on government in one way or another for basic services such as ID enrollment, and obtaining birth and death certificates.

Taxation

To develop a long-lasting economy and to provide public services, governments rely upon levying direct and indirect taxes on its citizens as well as businesses. Direct taxes are levied on the income of an individual citizen or a business. Indirect taxes are levied on goods and services in the form of duties. The global market size of sales tax software is expected to reach an estimated USD 11.25 billion by 2026.

As-is scenario

Taxation is considered one of the prominent revenue streams for the majority of governments in the world. During the 2018-2019 financial year in India, the Central Board of Direct Taxes (CBDT) reportedly collected around 11.17 lakh crores in Indian Rupees (INR). Although this figure seems staggering, it has been reported that the collected amount is still in a shortfall of around 83,000 crores, accounting for nearly 7.4% of the collection target that had been set. Similarly, indirect taxes will also be collected at the point of service. The amount of indirect tax collected may directly depend upon the state of the economy, wherein the buyer has enough purchasing power to afford a product or service. The medium of payment can also directly affect the collection of indirect taxes, as it becomes extremely difficult to trace cash transactions taking place in every nook and cranny of the country.

Let's look at the top issue faced by governments in taxation:

Evasion: Tax collection may decrease severely in situations where the service rendered to a customer is not recognized through a taxable sales invoice. Unfortunately, this may still occur if the customer and service provider mutually agree on exchanging the cash for service, thereby evading the payment of taxes.

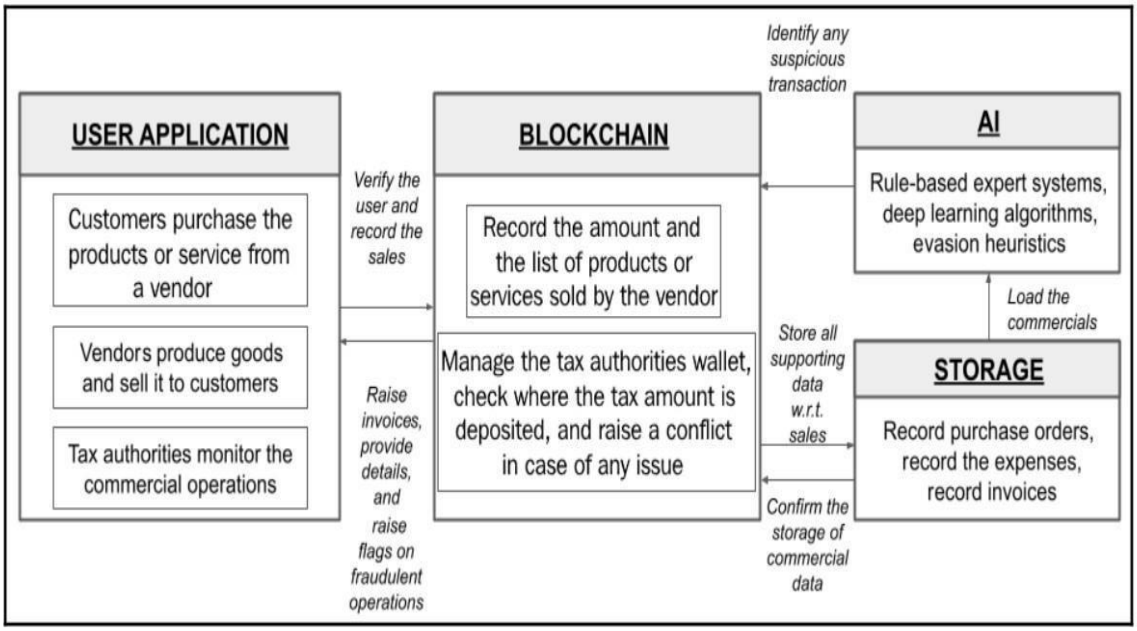
To-be scenario

In the future, businesses could be encouraged to use a blockchain-enabled application that keeps track of all inventories in the form of a Non-Fungible Token (NFT) to distinguish between the raw materials in a distinctive manner. Service providers could be compeled to transfer or account for the said NFT in the blockchain network. This can help identify the input and output of the item in the inventory and track the movement of goods across multiple stakeholders. Based on the transfer or sale of such resources, an invoice can be automatically generated by the smart contract and the customer asked for payment. By onboarding the entire supply chain process and sales life cycle on top of a blockchain, we may be able to curb indirect tax evasion significantly.

Possible solution

You may use any blockchain network to establish a public or a permissioned network, governed by the business owners as well as concerned tax authorities. All the incoming raw materials can be considered as inputs, with an NFT assigned to each unit of the raw material. Later on, once the product is manufactured from the raw materials, the corresponding NFTs could be burned and a new NFT created that is a composite of all the NFTs belonging to the raw materials used in the product. The sale of the product is now an auditable record persisted on the network, with a clear relationship establishing the composition. This will not only make the recording of input and output taxes easier, but it will also enable more tax collection along the way.

The following diagram summarizes our approach in a compartmentalized reference structure to help you understand the solution better:


USER APPLICATION
Customers purchase the products or service from a vendor
Vendors produce goods and sell it to customers
Tax authorities monitor the commercial operations
Verify the user and record the sales
Raise invoices, provide details, and raise flags on fraudulent operations
BLOCKCHAIN
Record the amount and the list of products or services sold by the vendor
Manage the tax authorities wallet, check where the tax amount is deposited, and raise a conflict in case of any issue
Identify any suspicious transaction
Store all supporting data w.r.t. sales
Confirm the storage of commercial data
AI
Rule-based expert systems, deep learning algorithms, evasion heuristics
Load the commercials
STORAGE
Record purchase orders, record the expenses, record invoices

Reference solution architecture to reduce tax evasion

As shown in the preceding reference solution architecture diagram, the suggested solution is split across four components, namely:

User application:

Unlike the solution architectures proposed previously, we have three main actors in this use case. There could be one application that can be used by end customers that allows the purchasing of finished goods at a retail level. There could be another application that allows vendors to sell raw goods among one another and also sell the finished goods to an end user. All the goods sold by users can be an NFT on a blockchain network such as Ethereum. While the sales are made, there could be a need for a dedicated application used by the tax authorities to monitor the B2B and B2C transactions in a pseudonymous format. Each sale can be drilled down as each can be recorded as a transaction on the blockchain with a rich context of supporting documents made available on a secondary network.

Blockchain:

The blockchain network will provide wallets to all three actors. Customers require a wallet in order to pay for the product or service. Vendors need the wallet to perform business and receive the quoted amount. The tax authorities need a wallet in order to transfer the indirect tax amount deducted at the point of sale. Vendor wallets will not only persist rupees or other local currencies, but also persist the balance of raw materials they have in stock. This balance is designated in a unique manner to each unit of the raw material. Once the raw material is converted into a finished product, the NFTs can be burned to mint a new NFT that can represent said finished product. Whenever a sale occurs between a customer and vendor (B2C), or among vendors (B2B), each sale is recorded as a transaction on the blockchain network, triggered by the payment action in the respective application.

Storage:

We need a decentralized storage service that can persist the paper trail of this process, ranging from purchase orders to invoices. We need an IPFS-based permissioned network that respects company privacy, and yet remains useful in sharing relevant data with authorities. Every time a paper document has been added to a vendor account, a new transaction bearing the relevant priority will be emitted in the network. Only eligible actors in the network should be able to view the transaction. This is an essential part of the design, so as to preserve the competitive spirit among all participatory stakeholders in the market.

AI: Now that we have the paper trail as well as the ledger balance, we can run rule-based expert systems to identify the tax amount to be collected. In order to identify any missing tax goals, we also need to use heuristics to identify potential evasion. Deep learning can also be employed to identify any money laundering activities.

Voting

Elections are regarded as a celebration of democracy, wherein each citizen is given the opportunity to exercise their rights in choosing the right representative to assume office. Hence, it is crucial that elections are held in an apolitical manner, without favor for any candidate or party. Also, it is beneficial to observe the latest changes in the technology community and apply the relevant technologies for the efficient and fair conduction of elections.

As-is scenario Currently, the majority of elections take place offline, meaning citizens are expected to enroll themselves and vote at a specified polling booth announced by the respective election authorities. This traditional process is regarded as outdated by a number of people. Based on the growing reach of the internet globally, a customer can place a purchase order on any e-commerce website to avail a product or service. Similarly, it may be convenient to allow citizens to vote from home or the office using their own mobile phones. This not only enables easier access to voting through a digital platform, but also reduces the time taken to announce the election results from days or hours to near-immediate.

The top issue faced by government in voting is as follows:

Speed up results: Many democratic nations offer holidays for citizens, to ensure that people are available to show up at the local constituency office, cast their votes, and then await the results. Although governments can facilitate voting, the process is largely a manual one. Hence, it takes time to handle, transfer, verify, and count all the votes at a designated secure location, a process that involves a lot of resources.

To-be scenario

In the future, governments and citizens should be encouraged to vote for their candidates using secure mobile applications that can be very simple to use. Each vote is cast by applying the citizen's private key, which could be resolved into a biometric signature, thereby proving the presence of the citizen during polling.

Possible solution

You may build a sample voting application on a mobile device or the web that communicates to a smart contract deployed on a blockchain network. The vote can be cast by each user by proving ownership of the private key associated with said account. Also, the application could leverage several pattern recognition techniques and computer vision to identify whether the person in front of the mobile device or the browser is a real person, and not a system-generated graphic. This can be made possible by using Generative Adversarial Network (GAN)-based classifiers. Once the votes are cast, we can double check the numbers and announce the winners of a hypothetical election.

The following diagram summarizes our approach in a compartmentalized reference structure to help you understand the solution better:

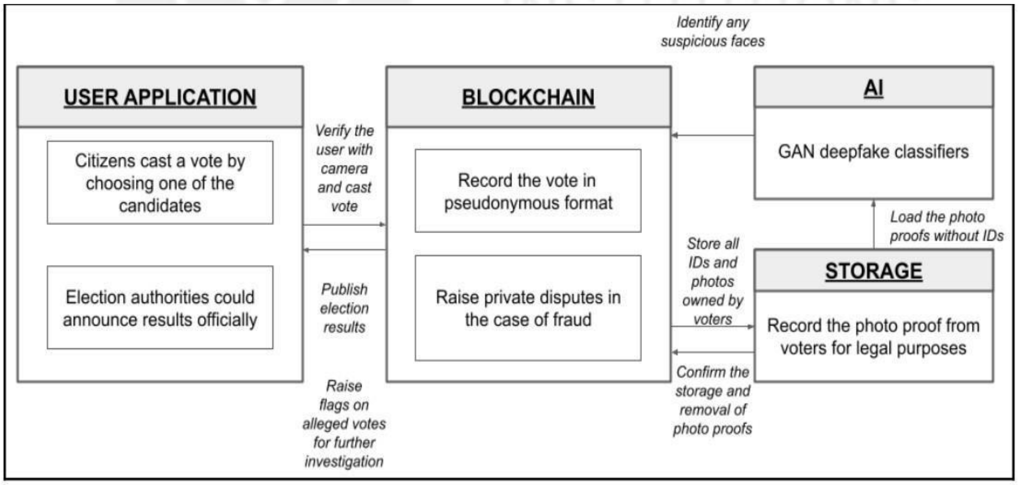

USER APPLICATION
Citizens cast a vote by choosing one of the candidates
Election authorities could announce results officially
Verify the user with camera and cast vote
Publish election results
Raise flags on alleged votes for further investigation
BLOCKCHAIN
Record the vote in pseudonymous format
Raise private disputes in the case of fraud
Identify any suspicious faces
AI
GAN deepfake classifiers
Load the photo proofs without IDs
Store all IDs and photos owned by voters
Confirm the storage and removal of photo proofs
STORAGE
Record the photo proof from voters for legal purposes

Fig 9.7: Reference solution architecture to reform election technology with a view to saving time and costs

Reference solution architecture to reform election technology with a view to saving time and costs

As shown in the preceding reference solution architecture diagram, the suggested solution is split across four components, namely:

User application: There could be one mobile application that could be used by citizens or users. This application must be tightly bound to one SIM in order to prevent Sybil attacks. This client application also needs to be able to capture the photo ID followed by a video of the poller in order to ensure that the vote is being cast by said person only. Similarly, there could be one web application or dashboard to monitor overall voter turnout and also to handle suspicious votes. The web dashboard can also provide topline information on the votes polled against each participant or candidate.

Blockchain:

The blockchain network will provide wallets for every single citizen or user. Votes are cast in a smart contract where mapping exists to count the votes made for each candidate. The blockchain can also be used to provide conflict management in case the AI identifies or warns of a false proof provided by a user.

Storage:

We require a decentralized storage service that can store the photo proof that can serve as legal evidence of the participation of users during the vote. It is very important to note that the video is uploaded by the respective citizen, another self-declaration on the part of the participant. Such data must be stored on an IPFS-based network in order to ensure that the data cannot be corrupted.

AI:

Now that the photo ID proof and the video of the citizen or user is made available, we can use the APIs of any IPFS-based network in order to vet the proofs shared with the authorities. With the recent release of GAN-based deep fakes, we can consider future-proofing this sample application by using advanced classifiers built on top of GANs only.

Legislative reforms

Legislation reforms are one of the key result areas of a government. Although bills are passed into acts, the enforcement of these acts may not be effective on occasion. Many reforms result in changes to financial planning, endorsements, and entitlements. One such example is social security. There may be one or several acts passed by a governing body that may require immediate and swift adoption. In such cases, we need to be able to ensure that the beneficiaries of these reforms are able to enjoy their benefits without a significant delay. As-is scenario Social security reforms, such as an increase in pension levels, may take time to be reflected on the checks. This transition may take time and not necessarily maintain transparency.

We can address this issue of social security reforms once suitable legislation has been passed. The top issues faced by governments in managing legislative reforms are as follows:

Enforcement:

Updated rules of law are seldom notified and acknowledged by common citizens. This information gap could create problems. Also, we need to make sure that the updated surplus amount is not pocketed by anybody across the value chain.

Documentation:

Once the legislative branch of government makes plans for an amendment, all the relevant documents must be tethered under a single repository. This will aid all members in reaching a common understanding regarding the background, objectives, and goals of the bill.

To-be scenario

In the future, governments could encourage the use of blockchain and AI to tackle numerous problems during legislative reforms. Also, AI could be used to detect any anomalies in the functions of the beneficiary and the benefactors. AI could also be used to identify any misappropriation of funds by employing deep learning techniques.

Possible solution

You could use any suitable blockchain platforms to record the votes on a proposed bill. You could also use blockchain to manage pension funds by locking and unlocking them based on a certain set of conditions. The blockchain platform could also identify each beneficiary by means of a wallet and utilize AI-based face recognition models to ensure that the funds are received safely by the respective beneficiaries.

The following diagram summarizes our approach in a compartmentalized reference structure to help you understand the solution better:

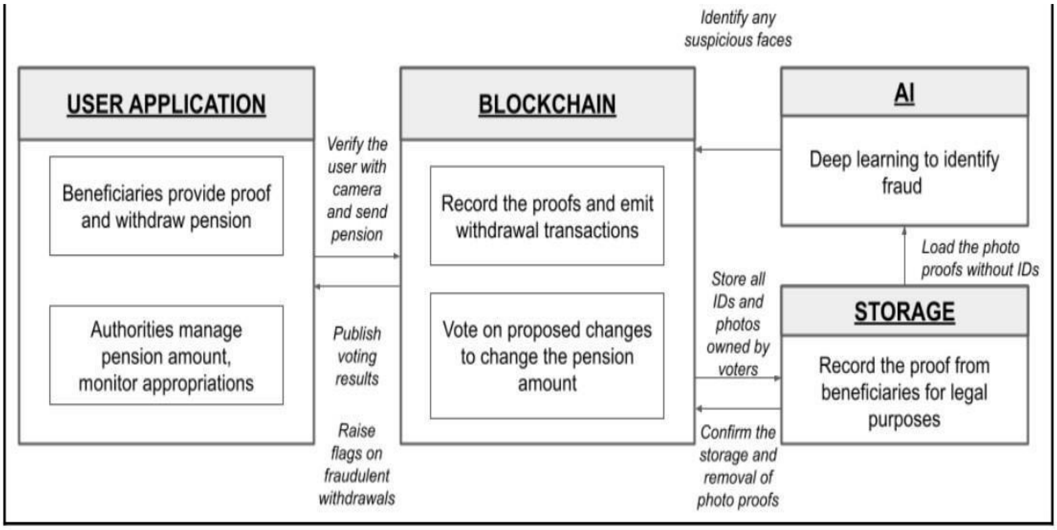

USER APPLICATION
Beneficiaries provide proof and withdraw pension
Authorities manage pension amount, monitor appropriations
Verify the user with camera and send pension
Publish voting results
Raise flags on fraudulent withdrawals
BLOCKCHAIN
Record the proofs and emit withdrawal transactions
Vote on proposed changes to change the pension amount
Identify any suspicious faces
Store all IDs and photos owned by voters
Confirm the storage and removal of photo proofs
AI
Deep learning to identify fraud
Load the photo proofs without IDs
STORAGE
Record the proof from beneficiaries for legal purposes

Fig 9.8: Reference solution architecture to rapidly support legislative reforms in social security

Reference solution architecture to rapidly support legislative reforms in social security

As shown in the preceding reference solution architecture diagram, the suggested solution is split across four components, namely:

User application:

There could be one form used by citizens, who are the entitled beneficiaries of the social security programs. There could be another form used by government agencies and the legislative house in order to vote on any changes and to also monitor appropriation of the funds in an open environment.

Blockchain: The blockchain network will provide wallets for each beneficiary as well as legislators. It will also host two separate contracts: a voting contract can be used to facilitate voting for and against the bill. A pension contract can also be used to facilitate the transfer of funds designated to the respective beneficiaries upon the set conditions. The beneficiaries could simply prove their existence in order to avail themselves of the pension.

Storage:

We require a decentralized storage service that can store the aforementioned proofs. These proofs may be required as a legal document for authorities. The proofs will be owned by the users and could be shared with authorities for a predetermined amount of time, in order to check for potential fraud or any other edge cases. Permission may be relinquished by the authorities once the proof is verified.

AI:

Now that we have proof of the existence of beneficiaries safely stored on an IPFS-based network, we could feed them to GAN-based classifiers and deep learning algorithms to identify any suspicious activity. Any suspicious or fraudulent transaction could be flagged by the model for dispute resolution with a backend team, where human effort can be involved.

Census

A census is a planned and articulated process organized by governments to calculate the latest population count in any given area. A census is also helpful in identifying the cultural and economic diversity of a particular area. As you may already know, a census is carried out every 10 years in India. The latest census was organized by the government of India in the year 2011, and it resulted in observing the latest population of 1,210,193,422 people.

As-is scenario

The government of India is organizing the 16th census during the year 2020-2021 with a key differentiator. The census operations will be digital, all driven through a mobile interface. Enumerators are given the option to either use the mobile app, or opt in for traditional paper-based record keeping, which are then submitted for digitization.

The top issues faced by governments in conducting a census are as follows:

Time to results:

Although the submissions made by enumerators could be digital, some manual efforts may be required to verify the authenticity of the data recorded by the enumerators. Also, it is imperative to reduce the time associated with verification, which could directly affect the turnaround time required to publish results.

Transparency:

The census process is all about knowing changes in terms of the cultural, social, and economic diversity of a region. As a community, it is a healthy and recommended practice to establish certain basic parameters and process checkpoints that could be published in an open network to address everyone's curiosity.

To-be scenario

In the future, census operations should not only go digital, but also emphasize the basic practices that enable communities to understand themselves in a fair manner.

This can be made possible by using public blockchain networks to communicate progress transparently.

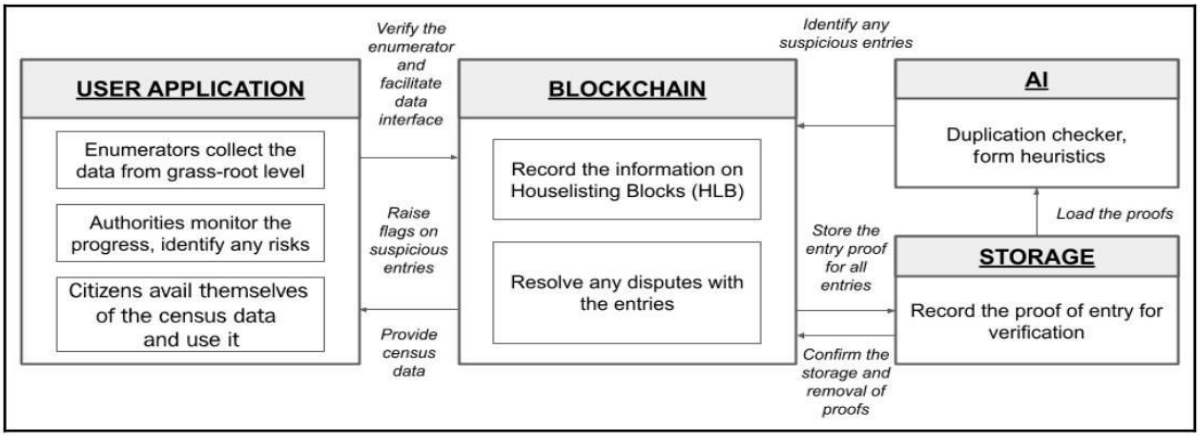
Future census operations could be powered by AI, in order to save costs and gain insights about the communities by drilling down on the large amounts of data collected.

Possible solution

The application can use a suitable blockchain to record and communicate all the checkpoints in the census operations. Blockchain wallets coupled with decentralized data stores can also be used to ensure that the information collected by enumerators at ground level cannot be reproduced in another medium.

The application can also leverage visualization tools and deep learning models that allow agencies and interested third parties to drill down on the accumulated data for demographic insights.

The following diagram summarizes our approach in a compartmentalized reference structure to help you understand the solution better:


USER APPLICATION
Enumerators collect the data from grass-root level
Authorities monitor the progress, identify any risks
Citizens avail themselves of the census data and use it
Verify the enumerator and facilitate data interface
Raise flags on suspicious entries
Provide census data
BLOCKCHAIN
Record the information on Houselisting Blocks (HLB)
Resolve any disputes with the entries
Identify any suspicious entries
Store the entry proof for all entries
Confirm the storage and removal of proofs
AI
Duplication checker, form heuristics
Load the proofs
STORAGE
Record the proof of entry for verification

Reference solution architecture to introduce a safe and transparent digital census As shown in the preceding reference solution architecture diagram, the suggested solution is split across four components, namely:

User application: There are three actors in the proposed system: enumerators, the census authorities, and the citizens of the country. To build this sample project, I am recommending three different forms. One form is used by the enumerators, who collect the data from every home at a grassroot level. The second form will be used by authorities to monitor the progress of the census operations and resolve any disputes with any suspicious entries. The third form will be used by common citizens who are interested in understanding about the cultural, economic, and demographic aspects of our society.

Blockchain:

The blockchain network will facilitate a wallet for each enumerator. The enumerators will receive a designated wallet address to be used while signing on entries in their app. Since each wallet is unique, it helps maintain accountability in the process. Each entry is a transaction with a signed message representing a hash of data added to the IPFS-based network.

Storage:

We require a decentralized storage service that can persist the information of all the citizens in a manner that ensures privacy. Proof of suspicious entries can be retained and access to the remaining entries relinquished.

AI: Now that the proof of entry is made available on an IPFS-based immutable record keeping network, we could use several supervised machine learning algorithms to detect duplicate entries. We could also use form heuristics in order to assess the quality of the data and compare between several Houselisting Blocks (HLBs). HLB is a term used widely in the census domain to identify a specific geographic habitat area. Each enumerator is allotted one or more HLBs to perform the census and submit all the required information.

Converging AI and blockchain in financial services

The financial services industry provides the economic backbone for institutions, organizations, and individuals to operate in a well-defined digital environment today.

Although financial services maintain a good reputation as one of the earlier adopters of all technologies, the same may not apply to the blockchain technologies. This may be due to the complications that arise from the transparency achieved in the process. However, we must understand that the application of blockchain with AI is almost inevitable at this point because most tech companies are starting to provide banking and insurance solutions to customers.

This is clearly disintermediating people from traditional banks and insurance companies.

Insurance

The market size of insurance software is growing at a rapid rate. There is quite a lot of diversification we may find in the insurance industry. With the latest coronavirus COVID-19 outbreak, there is a multifold increase in demand for health insurance all over the world.

As-is scenario

We are living in a world of Volatility, Uncertainty, Complexity, and Ambiguity (VUCA) with a dire need to afford protection from various unintended consequences. It may be interesting for you to learn that insurance is not limited to humans, animals, organs, and vehicles. Nowadays, you also find that smart contracts on several blockchain networks are also being insured, to protect against hacking or misuse. Hence, it is important to revisit how insurance management is operated today vis-à-vis a tech-enabled digital process of the future.

One of the top issues faced by insurance industries is as follows:

Claims management:

The process for making a claim may become complicated, based on the circumstances of the admission and the nature of the illness or accident. This calls for drastic measures in managing claims.

To-be scenario

In the future, hospitals and insurance companies could consider working closely in order to reduce costs and cut down on the time to process a claim. Hospitals, diagnostic centers, and insurers could form a consortium, create tokens, and settle using the same tokens for liquidity. Given the dire situation associated with a pandemic outbreak, we need to identify the best mechanisms to sustain. Let's explore a solution approach that could help better in managing claims.

Possible solution

If the patient is being admitted to hospital for treatment, this event could be recorded on the blockchain with the zero-knowledge proof, without giving away the personally identifiable information to anybody.

Perhaps a simple biometric signature could be of help here. Once the medical procedure is over, there could be a regular medical check by devices that can directly communicate with the blockchain and establish provenance at several levels.

Also, several AI-based advanced techniques can be leveraged to identify any fraud claims. It is a notable effort if insurance companies can expect doctors or any relevant certifiers to stake money on the blockchain before allowing them to approve any claims.

This could also significantly reduce the losses arising from fraud claims. In case a claim is known to be fraud, the insurance of the buyer could be barred, and the stake of the doctor or certifier could be liquidated, thereby rendering them non-functional.

The following diagram summarizes our approach in a compartmentalized reference structure to help you understand the solution better:

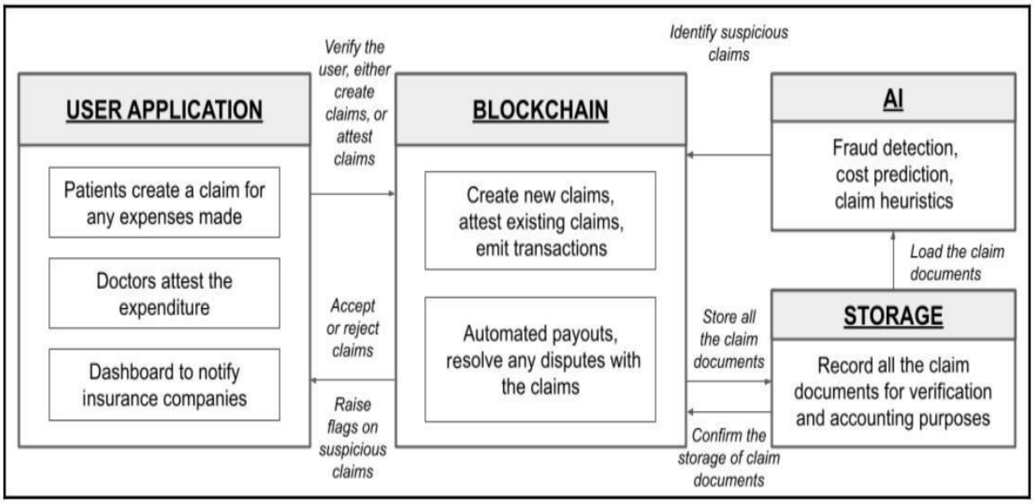

USER APPLICATION
Patients create a claim for any expenses made
Doctors attest the expenditure
Dashboard to notify insurance companies
Verify the user, either create claims, or attest claims
Accept or reject claims
Raise flags on suspicious claims
BLOCKCHAIN
Create new claims, attest existing claims, emit transactions
Automated payouts, resolve any disputes with the claims
Identify suspicious claims
AI
Fraud detection, cost prediction, claim heuristics
Load the claim documents
STORAGE
Record all the claim documents for verification and accounting purposes
Store all the claim documents
Confirm the storage of claim documents

Fig 9.10: Reference solution architecture to optimize the health insurance claim process for transparency and accuracy

Reference solution architecture to optimize the health insurance claim process for transparency and accuracy

As shown in the preceding reference solution architecture diagram, the suggested solution is split across four components, namely:

User application:

In this use case, I am suggesting three different apps. One app is to be used by customers or patients who have purchased insurance. They can fill out a form and attach the requisite information in order to successfully create a claim. The second app is suggested to be used by the resident doctors who treated the patient. Every time a new claim is created, the doctor is requested to verify and attest the claim. It is important to understand here that the doctor needs to stake a significant portion of their salary in order to perform attestation. In case the system identifies that the doctor had attested a fraud claim, the stake will be liquidated. The third app is a dashboard application suggested for insurance companies in order to monitor the topline information, such as the total payouts made in the past 24 hours, along with suspicious claims made in the past 24 hours.

Blockchain:

The blockchain network will provide a wallet for insurance companies to manage their funds. Users can pay their premium and expect the payout from such a wallet. The network will also provide a wallet to the doctor, in order to allow them to stake a significant portion of their salary in it. The same wallet could be used to remunerate doctors in case of valid claims. Finally, the network also needs to provide wallets for consumers or patients. They will receive payouts in the wallets. Notably, the blockchain network also needs to facilitate automatic payouts to eligible claims with the help of a smart contract. The validity of the claim will be decided based upon the supporting documents attached to the claim.

Storage: We require a decentralized storage service that can store all the supporting documents related to the claim. Once the documents are persisted, we could use relevant AI models and techniques to validate claims and also identify potentially fraudulent claims. We need to use any IPFS-based network in order to store these documents in an immutable manner so as to prevent any changes to the bill amount, dates, and other details.

AI:

With the critical claim-related documents stored on a secondary storage network, we could use a rule-based expert system to validate the claim structure and formats. We can also use machine learning techniques to identify any duplication in claims and also identify similar patterns to contrast the costs. If the conditions are satisfactory and below a programmed level of risk, an automated payout can be triggered. If the pattern observation looks suspicious, the models can post about the claim on the network in order to vote and resolve the claim issues.

Converging AI and blockchain in human resources

Hiring new talent and retaining existing talent has become one of the crucial agendas for organizations of all sizes. At the time of writing, the unemployment rate of the United States of America has been one of the highest since the last decade. This unprecedented rate of unemployment can be attributed to the COVID-19 outbreak. As the economy recovers, hundreds of thousands of new jobs will be created across multiple public and private sector organizations over the next few years. Although the opportunity for employment is growing at an exponential rate, there is also a difficulty in identifying the right talent who can match skills with salary. Especially in the tech domain, it is becoming extremely difficult to manage talents at two levels:

Retaining existing talent: This means that current employees are jumping companies in favor of a higher salary and better perks. This can be mitigated by a positive company culture accompanied by attractive salaries.

Onboarding new talent: This means that it is becoming difficult to hire new people who have entered the industry very recently. This can be mitigated by refining existing traditional processes to identify potential hires.

Although other industries may equally deserve a new breed of talent, let's limit the scope to our IT industry. In the following section, we will see how to address the issue of performing background checks on some critical technical resources in the IT industry.

Issues:

Background checks

Background checking is a process of formally verifying the information furnished by a job applicant. It is a process carried out by human resource managers and may vary in terms of when the process is carried out. Some companies and HR managers perform background checks after the applicant is successfully hired. However, there are a few companies that demand strict compliance of the background checks prior to confirmation of the application. The following are some of the common documents required during the background checking process:

Criminal documents:

Some companies may be required by law to check and verify whether an applicant has committed any criminal act. Such documents are accessed by respective law and enforcement offices of the land. Once it is confirmed that the applicant has not been involved in any criminal proceedings, the company may confirm the hiring of the candidate.

Financial documents:

Some companies may require the applicant to confirm the current salary offered by the existing role at the company. This could be verified if financial documents, such as bank statements, are furnished by the applicant. Drug test: Some companies may have strict policies against the abuse of drugs, and hence may require the applicant to undergo a drugs test. Based on the results of this test, the applicant may be confirmed or rejected on the grounds of company policies or the rule of law, as applicable.

Physical fitness:

There are a few jobs in government agencies across the world that may require a strict adherence to a few physical fitness criteria. Hence, the companies may require the candidate to undergo a new physical fitness test. Based on the results of the physical fitness test, the employer may make suitable decisions.

Previous work history:

Employers are usually required to maintain a record of the employment history of all of their employees. Employers may require a bona fide certificate from applicants, which may serve as certified proof. With a basic understanding of the background checking process and the common documents involved in the process, let's now understand the problems faced by the HR managers as well as applicants.

As-is scenario

Currently, most of the documents mentioned above are furnished by a job aspirant via email. The files sent by the applicant are received by the HR managers. It is worth pointing out that documents such as drug test results and physical fitness reports may be shared with HR managers internally by the third-party vendors who conduct the test. Some of the files pertaining to the applicant may contain sensitive and personally identifiable information.

The top issues plaguing the recruitment process and human resources management are as follows:

Lack of data ownership by the applicant: Most of the aforementioned documents are furnished by a job applicant via email. The files sent by the applicant are received by the HR managers. It is worth mentioning that documents such as drug test results and physical fitness reports may be shared with the HR managers internally by the third-party vendors who conduct the test. Some of the files pertaining to the applicant may contain sensitive and personally identifiable information.

Inability to perform strong automated background verification:

Once the documents are received by the HR managers, the documents go under scrutiny depending upon the company's policies. It should be noted that most of the verification efforts made by managers involve a manual process, meaning that this is time-consuming and may also be error-prone. Now that we have identified some of the vulnerabilities in the process,

To-be scenario

In the future, governments and companies should encourage the use of blockchain-based DIDs, to control the data that applicants share with employers. Applicants would be comfortable using a system wherein the data of the applicant could be redacted if they are not offered the job. Also, it is important to streamline the whole process with AI-enabled automation using Optical Character Recognition (OCR) for reading test results, and critical other documents such as financial statements. The applicant would be more comfortable if there is a specialized OCR program that can read the bank statement just to confirm the current salary of the applicant and immediately redact the document. This transformation in the background verification process will not only save the company time and money, but also provide for a more secure environment that could be applicant friendly.

Possible solution

We could use a suitable blockchain platform and build a smart contract that allows applicants to safely sign declaration forms with the company or the HR managers. Also, we can separate data from this process by allowing the applicant to store the data on a personal data storage medium such as MoiBit, so as to customize access to all the documents required by the employer in the process. We can also use OCR programs and carefully design a Zero-Knowledge Proof (ZKP)-based system that can confirm a number of attributes of the document without allowing the HR manager to access the data unnecessarily. The following diagram summarizes our approach in a compartmentalized reference structure to help you understand the solution better:

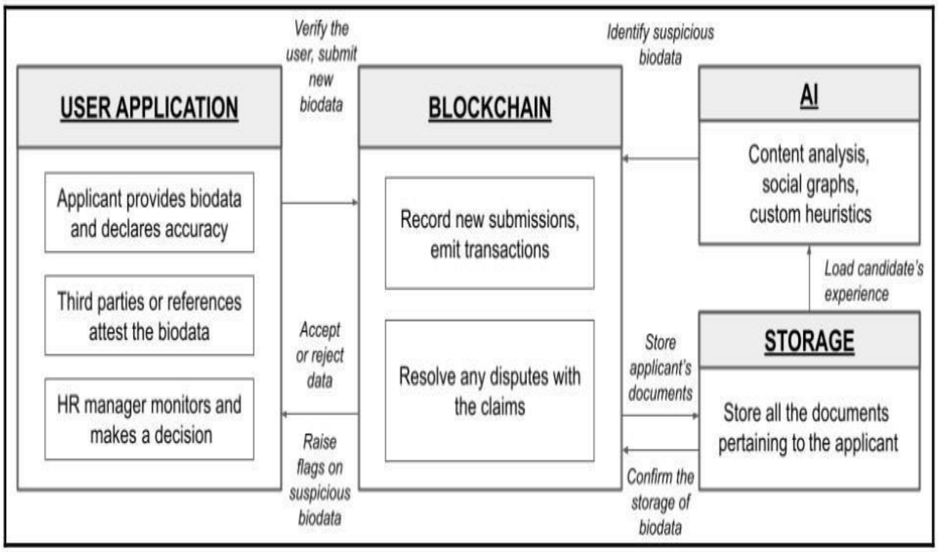

USER APPLICATION
Applicant provides biodata and declares accuracy
Third parties or references attest the biodata
HR manager monitors and makes a decision
Verify the user, submit new biodata
Accept or reject data
Raise flags on suspicious biodata
BLOCKCHAIN
Record new submissions, emit transactions
Resolve any disputes with the claims
Identify suspicious biodata
Store applicant's documents
Confirm the storage of biodata
AI
Content analysis, social graphs, custom heuristics
Load candidate's experience
STORAGE
Store all the documents pertaining to the applicant

Fig 9.11: Reference solution architecture to optimize the background checking process while interviewing a candidate

Reference solution architecture to optimize the background checking process while interviewing a candidate

As shown in the preceding reference solution architecture diagram, the suggested solution is split across four components, namely:

User application:

In this use case, it is suggested using three different applications. The first app can be used by applicants to apply for a company and share their biodata and all supporting documents already stored in their personalized data space. In this case, it is suggested using an IPFS-based network such as MoiBit, in order to provide access to users.

The second type of app can be used by third parties who perform drug tests and so on. It can also be used by previous employers and references in order to confirm the data declared by the applicant. Once the third parties or references provide information, it can be validated, and their efforts can be incentivized. However, in order to incentivize good actors, staking needs to be implemented.

Finally, the third type of application is used by HR managers to post job descriptions, shortlist candidates, review the automated verification results, and so on.

Blockchain:

The blockchain network will be used to provide wallets for all four actors: applicant, HR manager, references, and the third-party service provider. To prevent permanent access to information, we could use wallets and provide temporary read-only access to HR managers of prospective companies. Similarly, the efforts expended by the references and third-party service providers must be incentivized. Hence, wallets can be used to transfer to them directly tokens of their choice. Apart from the wallets, the blockchain network of choice should also be able to facilitate smart contracts to record updates to biodata. We can also use smart contracts to resolve the disputes in a public manner.

Storage:

We require a decentralized storage service that can store the biodata of applicants and share it with respective HR managers on demand. Each document stored by the applicant will be recognized on the network with a transaction.

AI: With the documents made available on a secondary network, we can validate the biodata with custom heuristics. We can also consider identifying the relevant references using social graphs. If anomalies are identified, we can have the system report it on the network for resolution. Following this detailed walkthrough of problems across several domains in the sphere of human resource management, let's now explore the problems faced by the healthcare industry.

Converging AI and blockchain in healthcare

The healthcare industry has transformed from an institutional system into a service-driven system enabled by many technologies. Many healthcare services, including diagnosis, treatment, and preventive medication, have become digital and engage with patients in a personal manner. Healthcare devices such as fitness bands, trackers, and medication pumps are replacing some of the medical personnel we rely upon. This transformation at the customer level can also be enhanced with the help of new drugs.

Some of the major issues faced by the healthcare industry.

Pharmacovigilance

Pharmacovigilance (PV) can be defined as a group of activities that includes various processes such as drug formulation, testing the newly formulated drugs, assessing the risks, and finally preventing any side effects from a drug before it can be introduced to the market. The main focus of pharmacovigilance is to ensure drug safety for consumers

These activities are carried out by many personnel and also require cross-industry stakeholders, under the careful oversight of the local drug administration agency.

Hence, there is a need for software that can facilitate these processes in a digital manner, reduce costs, and also identify any potential risks amid the testing based on the data available. Also, it is important that any adverse effect of using a drug is commonly reported to local drug administration authorities, as applicable.

Pharmacovigilance software is being used to report such cases. At the time of writing, the global market size of pharmacovigilance software is expected to exceed an estimated USD 250 million by 2027.

As-is scenario The basic requirements of any pharmacovigilance software could be to collect and assess data pertaining to drug experimentation. Another notable requirement for such software is to automate some of the processes and complement the need for human personnel. Such software is also expected to prepare well-defined and structured reports that are applicable under local regulations and the rule of law. Most of the successful pharmacovigilance software today offers flexible features to facilitate most of these requirements and cut down costs. There are several phases through which the safety of the drug will be assessed. The software is used to collect the reaction data, analyze it, and report it to applicable drug administration authorities. The software may also provide the insights needed to make the drug safer and reduce associated costs in the process.

The top issues faced by pharmacovigilance software are as follows:

Personal information of subjects:

People subjected to a drug trial are usually referred to as subjects. While subjects are undergoing such a trial, they are instructed to consume a prescribed amount of a given drug.

Drug consumption is monitored over a period of time to observe the reaction, understand more about the side effects, and gather useful information from the test. This information may be passed on to the drug formulation team to improve the product over the next iterations. During the course of testing, the subject may experience a number of adverse effects, including death. Local drug administration agencies may require the drug manufacturers to confirm such scenarios and debrief such adverse instances in a prescribed format detailing the cause. Due to the sensitivity attached to the personal information of the subject, not all the reporting data can be made accessible to the general public or other concerned authorities. The future of healthcare lies in the adoption of advanced transparency, which allows stakeholders to provide a larger exposure to such adverse data regarding a drug that may already be on the market.

To-be scenario

In the future, the local drug administration authorities may encourage the publication of all the adverse effect data in an anonymized manner, wherein each adverse situation faced by the subject under the drugs trial is briefed, but the personal identity of all those subjects who have experienced side effects is anonymized.

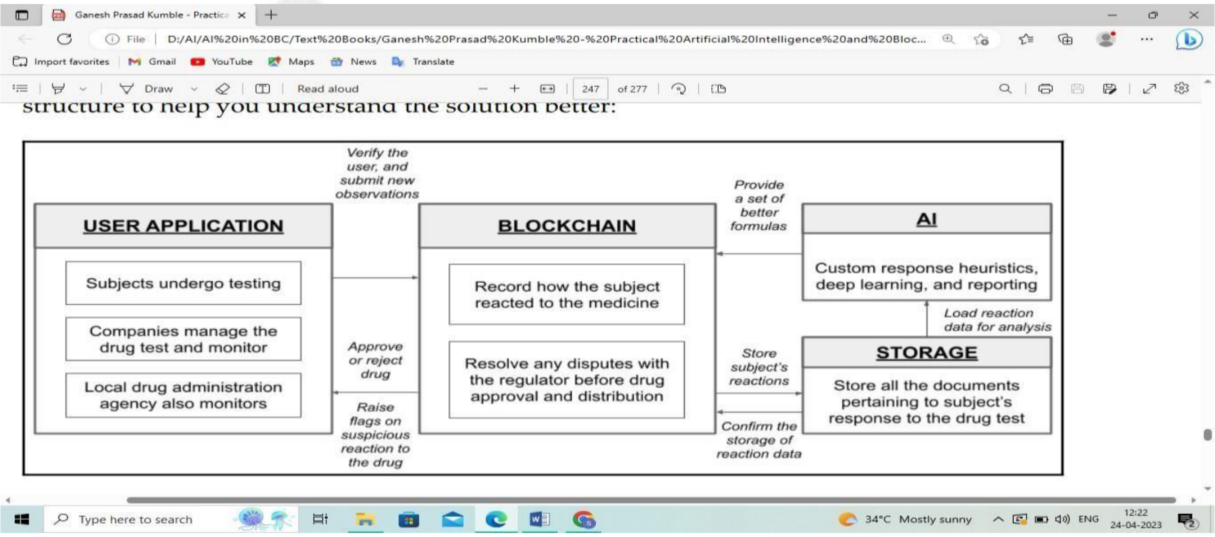
Here, blockchain can be used in pharmacovigilance software to establish transparency and provenance of the reports published by the respective stakeholders. AI can also be used to analyze critical data points from the reports and help confirm whether the adverse situations, such as the death of the subject, were caused by the drug alone, or other health conditions.

Possible solution

We can choose any suitable blockchain platform with the ability to handle the reporting of data in a public as well as a permissioned manner. There may be several reports strictly limited to a small number of stakeholders, thereby preventing the exposure of trade secrets.

Similarly, we can use AI models to predict any side effects during drug trials, since a third of subjects may suffer from a side effect as a result of drug-to-drug interactions.

The following diagram summarizes our approach in a compartmentalized reference structure to help you understand the solution better:



structure to help you understand the solution better:

Ganesh Prasad Kumble - Practic
File | D:/AI/AI%20in%20BC/Text%20Books/Ganesh%20Prasad%20Kumble%20-%20Practical%20Artificial%20Intelligence%20and%20Bloc...
Import favorites
Gmail
YouTube
Maps
News
Translate
Draw
Read aloud
247
of 277
Verify the user, and submit new observations
USER APPLICATION
Subjects undergo testing
Companies manage the drug test and monitor
Local drug administration agency also monitors
Approve or reject drug
Raise flags on suspicious reaction to the drug
BLOCKCHAIN
Record how the subject reacted to the medicine
Resolve any disputes with the regulator before drug approval and distribution
Provide a set of better formulas
AI
Custom response heuristics, deep learning, and reporting
Load reaction data for analysis
Store subject's reactions
Confirm the storage of reaction data
STORAGE
Store all the documents pertaining to subject's response to the drug test
Type here to search
34°C Mostly sunny
ENG
12:22
24-04-2023

Reference solution architecture to enable efficient drug approval and transparency in pharmacovigilance

As shown in the preceding reference solution architecture diagram, the suggested solution is split across four components, namely:

User application:

One application can be used by the subjects in order to upload the reaction to the drug along with suitable photos or vital information prescribed by authorities. The information will be stored under a pseudonymous wallet, without giving away too much personal information to the public.

There could be another application used by drug companies to review the reactions submitted by the subjects. This data can be very helpful to companies in formulating a better drug with lesser, or no, side effects.

Finally, we may need a separate dashboard for the local drug agencies to monitor any critical cases, report fatalities during drug tests, and also to approve or reject a drug.

Blockchain:

The blockchain network will provide wallets for all three actors: subjects, drug companies, and regulators. The drug reaction data will be safely shared to all three wallets. Also, it is important to maintain an auditable provenance of all the tests undergone by a drug. This may help future investigations and help identify the actors accountable. We will also need a smart contract in the network to facilitate the approval of drugs through a smart contract. This smart contract could simply run under the vigilance of a regulator, or showcase the collective interest of the group by digitally signing on the approval request transactions collectively, using the private keys of more than one wallets in the network. This approach is often referred to as multisig.

Storage:

We require a decentralized storage service that can store the exact unchanged version of the drug reaction from subjects. It is recommended using an IPFS-based network in order to customize access to the data.

AI:

Now that the drug reaction data is made available on an IPFS-based network such as MoiBit, we need to be able to use deep learning techniques and drug reaction heuristics. If a serious injury or fatality is identified, we can use the models to regenerate the drug formula to address the side effects.

Converging AI and blockchain in supply chain management

Supply chain management is defined as a group of activities that streamline the flow of all goods and raw materials that are required for the production of a finished good. It involves the storage and movement of raw materials, monitoring inventory, and the delivery of finished goods to the point of consumption. All these processes need to be digitally monitored and communicate any disruptions in real time. Hence, there is a need for intelligent supply chain management software that is flexible and accurate. The market size of supply chain management software is expected to reach a figure of around USD 25 billion by the year 2025. There are multiple approaches and solution architectures available for building intelligent Supply Chain Management (SCM) software.

The top issues faced by the supply chain industry and try to address their problems.

Volatility

Volatility can be experienced in the price of a commodity, due to a variation in supply and demand. Geopolitical issues, biohazardous issues, legal and other economic issues may also affect the price of a commodity. Managing the volatility of a commodity's price is a crucial element in supply chain management. Conversely, any risk arising from a supply chain could disrupt the price of commodities.

As-is scenario

The price volatility of goods in the supply chain may incur losses. Currently, supply chain stakeholders may incur these losses since the software may not be able to identify rapid changes in prices.

To-be scenario

In the future, supply chain stakeholders should form consortiums, identify liquidity problems in advance, and facilitate trade and logistics using blockchain and AI.

Possible solution

Blockchain platform can facilitate all the supply chain activities through a scalable smart contract support. It should be understood the capabilities of a blockchain and the volumes it can handle, before delving into the development aspects. This could help save time and effort before initiating the project. Also, consider using decentralized data storage options such as MoiBit to store all the critical paper trails necessary for maintaining audit purposes and establishing provenance. Finally, AI models could be developed to tap into the transparent ledgers to identify the current volumes of raw materials and make necessary arrangements for the same. However, if the supply is inhibited, the models could resort to hedging current raw materials in order to cover the surplus cost and carry forward with the operations.

The following diagram summarizes our approach in a compartmentalized reference structure.

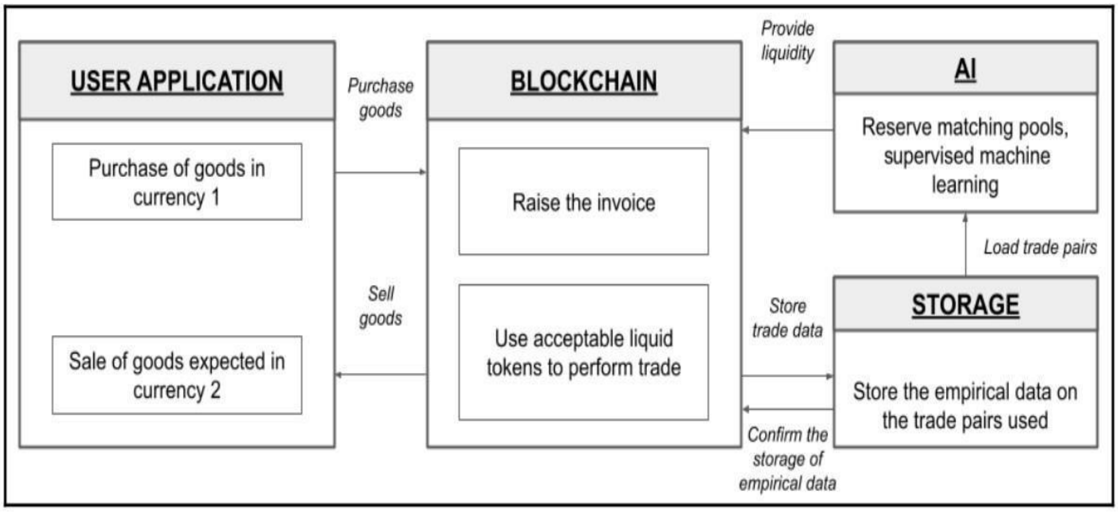

USER APPLICATION
Purchase of goods in currency 1
Sale of goods expected in currency 2
Purchase goods
Sell goods
BLOCKCHAIN
Raise the invoice
Use acceptable liquid tokens to perform trade
Provide liquidity
AI
Reserve matching pools, supervised machine learning
Load trade pairs
Store trade data
STORAGE
Store the empirical data on the trade pairs used
Confirm the storage of empirical data

Fig 9.13: Reference solution architecture to reduce volatility risks in supply chains and settle faster

Reference solution architecture to reduce volatility risks in supply chains and settle faster

As shown in the preceding reference solution architecture diagram, the suggested solution is split across four components, namely:

User application:

Simple application that can be used by buyers and sellers is proposed in the preceding diagram.

Blockchain: The blockchain network will provide wallets to the buyers and sellers. Instead of converting the local currencies to a global reserve, you can consider trading with custom stablecoins instead, which may be available in abundant numbers at lower conversion fees.

Storage: We require a decentralized storage service that can capture the trade pairs, without giving away the specifics of the trade. This can be made possible by persisting only those trade pairs that can be made available to anybody without harming anybody's privacy.

AI:

Now that the trade pairs are available, we can run supervised machine learning algorithms to optimize the search for finding traders who can sell stablecoins at a cheaper price. This could help reduce the volatility issues while converting the currencies, thereby reducing the overall time and cost required to settle.

Converging AI and blockchain in other domains

Law and order

The police department, local administration, and judiciary system work closely together in order to protect people from scams, violence, and other forms of criminal activities. This group of government agencies could collectively be referred to as law and order.

As-is scenario

Monitoring the actions of people, entities, and organizations in developing economies can be tedious with limited resources. We need to consider transforming some of the critical processes in our current system in order to maintain peace and grow businesses in the society.

The top issue faced by law and order authorities is as follows:

Conflict and arbitration management:

When an act is passed, it becomes challenging as a citizen to track and understand as to when said regulation will be applicable.

You may have also observed that although a rule of law has been passed by an upper house, it takes a significant time to see it materialize. Sometimes, a common rule of law may affect two or more government organizations, thereby leading to more confusion regarding the enforcement of said rule. These issues will result in a delay of service to citizens.

To-be scenario

In the future, law and order needs to strike a balance between the need for human intelligence in contrast to the efficiency offered by machines and networks. This can be made possible by tightly knitting our executive, legislative, and judicial branches. Optimizing the flow of a certain set of decision-making processes already occurring in a repetitive manner could help serve the community better. A consortium of government agencies could not only help the administration achieve the performance expected, but also bring down the costs of enforcement significantly. Let's now explore the issues faced in achieving national security and try to address their problems.

National security

National security is of the utmost importance for every country. For developing countries, efforts are made in order to ensure that they secure a better position in the global political arena. Similarly, developed countries may make efforts in ensuring that they do not lose their relatively higher position in the global political arena. Between these two aims lies the interest vested in potentially sabotaging the efforts of another country through proxy wars, internal political instability, and espionage.

As-is scenario

India's geo-political position is that of a relatively higher status compared to some of its adversaries. This is due to the geographical challenges faced by some of its adversaries and also the economic progress the country is making as a developed country. In the midst of such remarkable progress, we may encounter a few efforts to sabotage initiatives taken by the nation's administration. Hence, we must identify these issues and handle them in a suitable manner.

The top issue challenging the forces in addressing national security matters is as follows:

Unmanned Aerial Vehicles (UAV):

Many of these domestic drones that fly in the form of a quadcopter are referred to technically as UAVs. UAVs pose a threat to both civilians and the military. Hence, it is important to identify all the drones that are imported, operated, and destroyed in India.

To-be scenario

In the future, governments could encourage the authorities to enroll all the UAVs and any other supporting equipment with the help of a blockchain. Also, the agencies could set up a local UAV response center in each zone of the city in order to mitigate any live risk by the drones. These response centers could use AI-based techniques to analyze the feeds from radio sensors in order to predict any unscheduled flight of a UAV. This intelligence could help assess the risk of an attack before it takes place.

Environment conservation

It is a fundamental duty and a moral obligation to protect the Earth, our only home. One approach to protect the planet is through the conservation of our ecological diversity that contributes to the stability of our planet. Climate change is visible across several parts of the world in different ways. Although it may not be at devastating levels, it will soon reach an irreversible point of destruction. To prevent this from happening, we can try our best to conserve our wildlife and our ecological diversity on land as well as water.

As-is scenario

Currently, several greenhouse gases, including carbon monoxide (CO), carbon dioxide (CO2), and methane are prevalent in our atmosphere as a result of burning fossil fuels, cattle rearing, and the manufacture of a number of industrial goods.

The primary issue inhibiting energy conservation efforts is as follows:

Carbon pricing:

Carbon pricing is a method of reducing greenhouse gas emissions by charging a surplus on the fuels or setting an allowance on the quantity of gas that can be emitted by an entity. Under the Paris Agreement, many countries have already volunteered for carbon pricing. However, a few countries are yet to support the movement. Although many countries have already volunteered, it may become difficult to communicate the progress of this movement if the changes are not made visible in a transparent manner.

To-be scenario

In the future, all the countries who volunteer to join the Paris Agreement could log all the carbon offset data into the blockchain. This information may transition from the basic consumer to the supplier, all the way to governments and back to the Paris Agreement members who may also join the consortium.

Agriculture

Agriculture is the backbone of India's economy. It is one of the foremost contributors to our Gross Domestic Product (GDP), with a global market size estimated to reach nearly USD 12 trillion over the next 3 years.

As-is scenario

Over the past few years, the agriculture industry in India has been facing some serious issues. Aside from the distress faced by farmers due to irregular monsoons, floods, and famine.

The top issues plaguing the agriculture industry are as follows:

Fair price discovery for farmers:

With the advent of the internet, it was easier to discover prices through some of the co-operative systems that decide the price for the yield. Farmers were also able to discover the price of the yield from the neighboring markets. However, there could be a larger game at play if brokers plan on corroborating on a price that favors their personal motives. This is achieved by brokers sourcing the yield locally for a low price and exporting it to a market that may not be aware of the local yield price.

Instant lock-in and payments:

Even if farmers are okay with the price set by the brokers, there is no guarantee of instant payment once the yield is deposited at the warehouse. Once the yield is hoarded in the warehouse, the broker may find a suitable buyer, take the cut, and then make the payment back to the farmer. In India, this may take many days, or weeks. A farmer’s obligations may not be met in case payment is delayed. Some farmers have lost their assets, while others have resorted to suicide, a very sad state of affairs.

To-be scenario

In the future, all farmers should consider joining a price discovery app hosted on a blockchain network in order to share the price information of all yields at district as well as state level. Farmers should also consider trading the yields and collateralizing loans among themselves in the short term.

Assignments

Toppers:

Decentralized AI Marketplaces: Create a decentralized platform that connects AI developers and consumers using blockchain technology. This platform should facilitate the buying and selling of AI models, datasets, and services. Utilize smart contracts to automate transactions and ensure transparency and security in AI model exchanges.

Above Average:

Blockchain-based AI Data Market: Develop a blockchain-powered marketplace where individuals can securely buy and sell their data to train AI models. Implement privacy-preserving techniques such as homomorphic encryption or zero-knowledge proofs to enable data transactions without revealing sensitive information. Additionally, integrate AI algorithms to facilitate data matching and ensure fair pricing.

Average:

AI-driven Supply Chain Management on Blockchain: Design an AI-powered supply chain management system that leverages blockchain for transparency and traceability. Develop algorithms that analyze data from IoT devices, sensors, and other sources to optimize supply chain processes such as inventory management, demand forecasting, and logistics. Use blockchain to record and verify transactions, ensuring the integrity of supply chain data.

Below Average:

AI-powered Fraud Detection and Prevention using Blockchain: Develop an AI-driven fraud detection system integrated with blockchain technology to combat financial fraud. Train machine learning models to analyze transaction data in real-time and identify suspicious patterns indicative of fraudulent activity. Utilize blockchain to securely store and timestamp transaction records, enabling immutable audit trails and enhancing the accuracy and reliability of fraud detection algorithms.

Slow Learners:

Decentralized Autonomous Organizations (DAOs) with AI Governance: Construct a DAO governed by AI algorithms running on blockchain. Design AI systems capable of making governance decisions, such as resource allocation, voting mechanisms, and rule enforcement, based on predefined objectives and input from DAO participants. Implement smart contracts to execute AI-driven decisions transparently and autonomously.

Part-A Questions and Answers

1. **What are the technical challenges related to Bitcoin Blockchain (C05,K2)**

   Some of the the issues include increasing the block size, addressing blockchain bloat, countering vulnerability to 51 percent mining attacks, and implementing hard forks

2. **Define Throughput related to Blockchain (C05,K2)**

   The Bitcoin network has a potential issue with throughput in that it is processing only one transaction per second (tps), with a theoretical current maximum of 7 tps.

   One way that Bitcoin could handle higher throughput is if each block were bigger, though right now that leads to other issues with regard to size and blockchain bloat.

3. **List two security issues in Blockchain (C05,K2)**

- The possibility of a 51-percent attack, in which one mining entity could grab control of the blockchain and double-spend previously transacted coins into his own account.
- Another security issue is that the current cryptography standard that Bitcoin uses, Elliptic Curve Cryptography, might be crackable. However, financial cryptography experts have proposed potential upgrades to address this weakness.

4. **What are the five layers of the solution architecture (C05,K2)**

   Application layer, Presentation layer, Network layer, Data layer and Physical layer.

5. **What is the function of Application layer? (C05,K2)**

The application layer consists of end users and client software installed on mobiles, laptops, and devices.

6. **What is the function of Presentation layer? (C05,K2)**

The presentation layer consists of backend functionalities manifested in the clients, which are not visible to end users.

7. **What is the function of Network layer? (C05,K2)**

As the name suggests, the network layer consists of service networks consisting of blockchain validator nodes running a software bundle designated for verifying user transactions and blocks formed by other nodes in the blockchain network.

8. **What is the function of Data layer? (C05,K2)**

The data layer defines, persists, and provides the interface for applications to access user data, network data, and other processed data.

9. **What is the function of Physical layer? (C05,K2)**

The physical layer represents all the Graphics Processing Unit (GPU) nodes, virtual machines (VMs), and storage nodes used to store the data and perform complex computations.

10. **Define KPI**

Key Performance Indicators (KPIs), are used to identify any potential growth

or

pitfall in the business.

11. **What is the top issue faced in managing data security on the public cloud? (C05,K2)**

Granular access control and encryption:

Enterprise applications mostly handle critical information about the company's financial data, trade secrets, design files, and leads on a potential client. Due to the nature of the information being used and circulated, there is a need to be extra vigilant regarding the sharing of knowledge. In the wrong hands, leaked information about the company can result in devastating effects on the company's performance.

12. **What is the top issue faced by enterprises in finance management (C05,K2)**

Accounting scandals: An accounting scandal is defined as an intentionally orchestrated process of manipulating the financial statements of a company in order to achieve the purpose of deceiving someone.

13. **What is the top issue faced by governments in taxation (C05,K2)**

Evasion: Tax collection may decrease severely in situations where the service

rendered to a customer is not recognized through a taxable sales invoice. Unfortunately, this may still occur if the customer and service provider mutually agree on exchanging the cash for service, thereby evading the payment of taxes.

14. **What is the top issue faced by government in voting (C05,K2)**

Speed up results: Many democratic nations offer holidays for citizens, to ensure that people are available to show up at the local constituency office, cast their votes, and then await the results. Although governments can facilitate voting, the process is largely a manual one. Hence, it takes time to handle, transfer, verify, and count all the votes at a designated secure location, a process that involves a lot of resources.

15. **What is the top issues faced by governments in managing legislative reforms (C05,K2)**

Enforcement:

Updated rules of law are seldom notified and acknowledged by common citizens. This information gap could create problems. Also, we need to make sure that the updated surplus amount is not pocketed by anybody across the value chain.

Documentation:

Once the legislative branch of government makes plans for an amendment, all the relevant documents must be tethered under a single repository. This will aid all members in reaching a common understanding regarding the background, objectives, and goals of the bill.

16. **What is the top issues faced by governments in conducting a census (C05,K2)**

Time to results:

Although the submissions made by enumerators could be digital, some manual efforts may be required to verify the authenticity of the data recorded by the enumerators. Also, it is imperative to reduce the time associated with verification, which could directly affect the turnaround time required to publish results.

Transparency:

The census process is all about knowing changes in terms of the cultural, social, and economic diversity of a region. As a community, it is a healthy and recommended practice to establish certain basic parameters and process checkpoints that could be published in an open network to address everyone's curiosity.

17. **What is the top issues faced by insurance industries? (C05,K2)**

Claims management:

The process for making a claim may become complicated, based on the circumstances of the admission and the nature of the illness or accident. This calls for drastic measures in managing claims.

18. **What are the issues in human resource management? (C05,K2)**

Background checks

Background checking is a process of formally verifying the information furnished by a job applicant. The following are some of the common documents required during the background checking process:

Criminal documents:

Some companies may be required by law to check and verify whether an applicant has committed any criminal act.

Financial documents:

Some companies may require the applicant to confirm the current salary offered by the existing role at the company. This could be verified if financial documents, such as bank statements, are furnished by the applicant.

Drug test:

Some companies may have strict policies against the abuse of drugs, and hence may require the applicant to undergo a drugs test. Based on the results of this test, the applicant may be confirmed or rejected on the grounds of company policies or the rule of law, as applicable.

Part-B Questions

Q. No	Questions	CO Le	K Leve
1	Explain the hybrid architecture for developing DIApps	CO5	K2
2	Explain the five layers in the architecture for developing DIApps in detail	CO5	K2
3	Discuss the various technical challenges related to Blockchain in detail	CO5	K2
4	Explain the various technical challenges and the possible solutions in using Blockchain in detail.	CO5	K2
5	Explain business model challenges to be overcome in developing DIAPPs in detail.	CO5	K2
6	Explain the reference solution architecture for identifying security threats in ERP systems with the help of blockchain and AI	CO5	K2
7	Explain the reference solution architecture for managing expenditures and identifying any fraudulent transactions with the help of blockchain and AI	CO5	K2
8	Explain the reference solution architecture to reduce tax evasion wit help of blockchain and AI	CO5	K2
9	Explain the reference solution architecture to reform election technology with a view to saving time and costs wit help of blockchain and AI	CO5	K2

10	Explain the reference solution architecture for gamifying the user feedback system in order to increase the performance of a product or service with the help of blockchain and AI	CO5	K2

Supportive online Certification courses (NPTEL, Swayam, Coursera, Udemy, etc.,)

Supportive Online Certification Courses

Sl. No.	Courses	Platform
1	Blockchain Basics	Coursera
2	DeFi Decentralized Finance	Coursera
3	Blockchain	NPTEL
4	Blockchain and its Applications	NPTEL

Real time Applications in day to day life and to Industry

Uniswap

Launched in 2018, Uniswap is a US-based DApp on the Ethereum blockchain. The platform primarily allows users to swap and trade ERC-20 tokens. It is the most popular decentralized exchange and, overall, the fourth largest crypto exchange on the internet. The platform hosts more than 150k monthly users, with a $2.5 billion daily trading volume on average.

Perhaps the most special feature of Uniswap is that it does not rely on buyers and sellers to create liquidity. Anyone can access the platform by simply connecting a crypto wallet. For this purpose, the most common choice among Uniswap users is the MetaMask wallet. The exchange charges a flat 0.3% fee per trade, plus the Ethereum gas fee, which varies from time to time.

- **Aave**

Aave is one of the most popular DApps in the DeFi world. It is an open-sourced liquidity protocol, providing users with complete transparency. It allows users to lend, borrow, stake, and earn interest on deposits. Thanks to the decentralized nature of the platform, both lenders and borrowers can enjoy complete anonymity.

Probably the most important use of Aave is to carry out flash loans. These loans are conducted within a few seconds and are necessary for the DeFi space to optimize the overall financial structure. AAVE charges a 0.09% fee on flash loans.

Content Beyond Syllabus

Dapps in Healthcare Industry

Digital decentralization has opened doors to new possibilities in the health sector. Moving to a decentralized crypto-enforced data system has the potential to revolutionize the healthcare sector in tremendous ways.

1. Data exchange

The real-time information sharing among users is one of the best-selling points of decentralized applications in healthcare. Take prescribed medication as an example. While two patients may exhibit similar symptoms, different practitioners could use different treatments on them to achieve the same result. One prescription may be more effective than the other, but because both practitioners work without interaction, there's little way for one to learn from the other.

Decentralized apps promise to link hospital data systems across a shared network, so that the exchange of such information can happen in real-time, from one end to the next. If a hospital makes a prescription, the data would be updated automatically for everyone using the Dapp to see it. The same goes for patients visiting hospitals having undergone treatment elsewhere. The medical practitioner would be able to find out exactly what was administered to the patient before, and make an informed, accurate decision.

2. Data security

Although Blockchain and decentralization present their own security and privacy concerns, they offer a much safer paradigm for storing and distributing digital information; one that is a lot more robust against risks like hacker attacks than traditional data systems.

- Cybercriminals successfully target hospitals in part because they store most of their data in discrete and isolated central servers, which can easily be compromised. They exploit the existence of a centralized data management system to lock a hospital out of its own server.
- In a decentralized world, all information is distributed and shared across many points on the network, which means there’s no single point of failure. Hacker attacks would therefore become a lot more difficult.

3. Public health

- Having a decentralized network that connects numerous health practitioners and organizations which can prove very be very beneficial when dealing with epidemic cases. A shared, immutable and trustworthy stream of information about ongoing diagnostics could help to keep everyone on the same page at all times.
- Dapps could also facilitate the sharing of research, clinical trials, advanced directives and safety analyses, and therefore enhance collaboration.

4. Hospital administration

- Decentralized applications are poised to significantly streamline the communication among staff in health organizations. If all authorised workers in a hospital have direct access to data, they’ll be able to work under much less supervision. Keeping everyone in the loop regarding hospital operations will make administration, along with managing daily processes like patient verification and insurance claims much easier.

5. Managing patient data

- Perhaps the biggest potential of decentralized applications in healthcare is that they could empower patients to gather, own and manage their data, rather than having it stored in an EHR (Electronic Health Record) system that is out of their reach. Patients could use personal health devices like fitness trackers and IoT devices to record data and share it with medical practitioners in real time.

Assessment Schedule (Proposed Date & Actual Date)

Assessment Schedule

Assessment Tool	Proposed Date	Actual Date	Course Outcome	Program Outcome (Filled Gap)
Assessment I	14.08.2025	14.08.2025	CO1, CO2	
Assessment II	23.09.2025	23.09.2025	CO3, CO4	
Model	28.10.2025	28.10.2025	CO1, CO2, CO3, CO4, CO5	
End Semester Examination	20.11.2025	20.11.2025	CO1, CO2, CO3, CO4, CO5	

Prescribed Text Books & Reference

Prescribed Text & Reference Books

Sl. No.	Book Name & Author	Book
1	Ganesh Prasad Kumble, Anantha Krishnan, "Practical Artificial Intelligence and Blockchain: A guide to converging blockchain and AI to build smart applications for new economies", Packt Publications, 2020. (unit 1-5)	Text Book
2	Melanie Swan, "Block Chain: Blueprint for a New Economy", O'Reilly, 2015. (unit 5)	Text Book
3	Daniel Drescher, "Block Chain Basics", Apress; 1st edition, 2017	Reference Book
4	Salman Baset, Luc Desrosiers, Nitin Gaur, Petr Novotny, Anthony O'Dowd, Venkatraman Ramakrishna, "Hands-On Block Chain with Hyperledger: Building Decentralized Applications with Hyperledger Fabric and Composer", Import, 2018	Reference Book

Mini Project Suggestions

Toppers: AI-Powered Decentralized Identity Verification

Develop a blockchain-based identity verification system that utilizes AI algorithms for facial recognition, voice recognition, and biometric authentication.

Use smart contracts to manage identity records securely on the blockchain, ensuring data integrity and user privacy.

Implement machine learning models to continuously improve the accuracy of identity verification over time.

Above Average: AI-Driven Predictive Maintenance for IoT Devices on Blockchain

Create a system where IoT devices record operational data onto a blockchain.

Utilize AI algorithms to analyze this data and predict maintenance needs or potential failures of the IoT devices.

Implement smart contracts to trigger maintenance actions automatically when certain thresholds are met, ensuring proactive maintenance and reducing downtime.

Average: Blockchain-Based AI Marketplace

Build a decentralized marketplace where AI models, datasets, and services can be bought and sold using blockchain technology.

Employ smart contracts to facilitate transactions and ensure transparent and immutable records of ownership.

Use AI algorithms for matchmaking, recommending relevant AI solutions to buyers based on their needs and preferences.

Below Average: AI-Driven Energy Trading Platform on Blockchain

Develop a peer-to-peer energy trading platform that utilizes blockchain for transparent and secure transactions.

Implement AI algorithms to forecast energy supply and demand, optimize pricing strategies, and match buyers with sellers in real-time.

Use smart contracts to automate energy trading agreements and settlement processes, reducing transaction costs and eliminating the need for intermediaries.

Slow Learners: AI-Enhanced Blockchain-based Healthcare Data Sharing Platform

Create a blockchain-based platform for securely sharing and accessing healthcare data, with AI-driven privacy-preserving mechanisms.

Utilize homomorphic encryption or federated learning techniques to enable AI analysis of sensitive healthcare data without compromising patient privacy.

Implement smart contracts to manage access control and consent management, ensuring that data is only shared with authorized parties and in compliance with regulations like HIPAA.

Thank you

Disclaimer:

This document is confidential and intended solely for the educational purpose of RMK Group of Educational Institutions. If you have received this document through email in error, please notify the system manager. This document contains proprietary information and is intended only to the respective group / learning community as intended. If you are not the addressee you should not disseminate, distribute or copy through e-mail. Please notify the sender immediately by e-mail if you have received this document by mistake and delete this document from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.