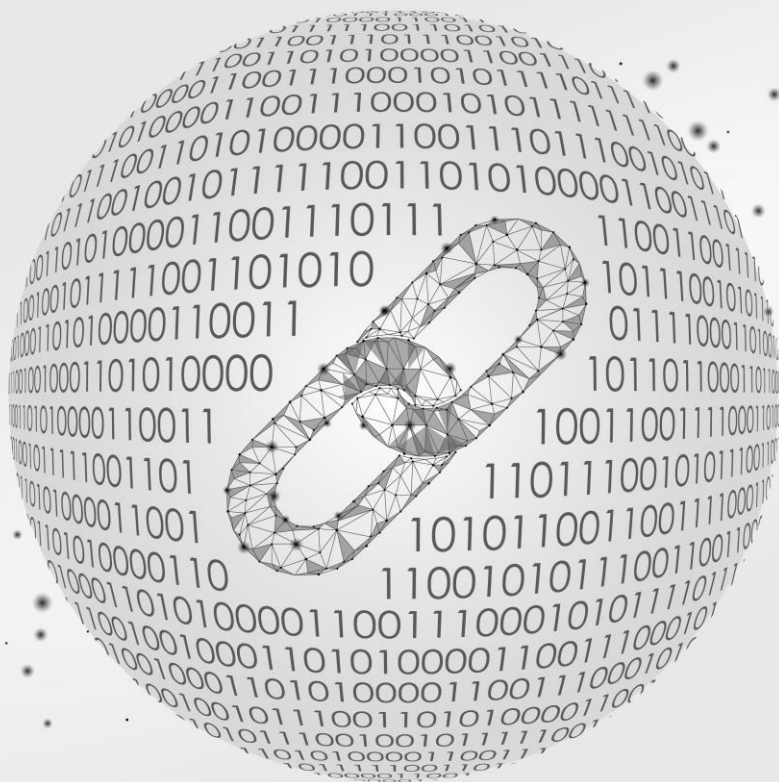




Zebi is founded, mentored and managed by Stanford, MIT, Oxford and IIT veterans and thought leaders from Silicon Valley with experience in Google, Uber, Amazon, Microsoft, and Oracle



Blockchaining India's Big Data

- Multi-year contract signed with an Indian state (50M population) government
- Proposals submitted to two additional state (160M population) governments
- Zebi Chain™ live in production
- Low hard cap of \$10M

WHITEPAPER FOR SALE OF ZEBI COIN

Table of Contents

Executive Summary	3
Important Notice	4
The India Opportunity	7
Background	8
What is happening with Big Data?	8
What is being done about it? And is it working?.....	11
Zebi Blockchain Solution for Big Data	13
Introduction	13
Bird's-eye view of the solution.....	13
Zebi Chain™	14
Zebi Data Gateway:	15
How Zebi Data Ecosystem will transform Industries	15
Status of Product and Market Development	19
Road Ahead	20
Zebi Coin (ZCO) Sale	21
Zebi Coin:.....	21
Tokensale Model:.....	21
Bonuses:	22
Additional Notes:.....	23
Team	24
Advisors	25
Additional Terms and Conditions	27
Country Specific Disclaimers and Restrictions	30
Risks and Uncertainties	31
References	35

Executive Summary

India's big data generation is increasing exponentially and is expected to reach 3 Zebibytes per year (1 Zebibyte = 1024^7 bytes, about trillion Gigabytes) by 2020¹, driven by continued growth of internet usage, social networks, proliferation of smart phones, as well as the digital initiatives and structural reforms undertaken by the Indian government. At the same time, incidents of data crimes such as data hacks, data leaks, data tampering, identity thefts are on the rise, which are costing Indian organizations and consumers more than \$30 billion² annually.

High value data like land registry, educational documents, employment, transaction and health records etc. are required by individuals and organizations as part of their routine activities. However, current mechanism of data exchange is mostly manual, paper based, slow and fraught with risks of tampering, forgery and thefts.

Governments worldwide are realizing the need to add stringent data regulations to safeguard people's interest with steep penalties for non-compliance. Examples are India Supreme Court Ruling on Privacy³, European Union GDPR⁴, Singapore's Personal Data Protection Act and India Privacy Bill⁵. However, enforcement of data protection regulations is still manual and are prone to manipulation.

Recognizing the need and opportunity to enable with technology the enforcement of data protection regulations, Zebi has created a Blockchain driven, unique and holistic solution to make high value and sensitive data readily available for legitimate use. Zebi safeguards data against hacking and tampering, while obtaining consent from individuals. The solution comprises of Zebi Chain™ to provide immutability to critical records, coupled with a central hub called Zebi Data Gateway which enables secure and instant data exchange through Data-as-a-Service (DaaS) APIs. Zebi's innovative, proprietary solution set is one of the first in industry and is patent pending. Zebi has developed the Zebi Blockchain Solution and is carrying out its operations through its affiliate Zebi Data India Pvt. Ltd. in India.

Integrated with Ethereum blockchain, Zebi Chain™ gives complete flexibility to customers with respect to private/public blockchain utilization. Smart contracts enabled on Zebi Data Gateway ensure that data exchange occurs only with consent and that all stake holder receive their deserved share of the data monetization. Accounting for the risks specified in this Whitepaper in the section titled "Risks and Uncertainties", This has the potential to transform broad range of industries: protection and verification of land registry, education, employment, transaction and health records, credit scoring, personalized marketing and fraud detection.

Zebi Chain™ has been well received by the market. Zebi, through its affiliate Zebi Data India Pvt. Ltd., recently signed a multi-year contract to implement Zebi Chain™ for one of India's largest state governments (with 50m population) to safeguard their land assets⁶.

Additionally, Zebi has a healthy pipeline of prospects across India and is prospecting through its affiliates for projects across Singapore, USA and other countries. Zebi Chain™ installations will be connected to Zebi Data Gateway, which will serve as the pipeline for authorized use of data for commercial purposes. If we are able to rapidly scale and add more Zebi Chain™ customers, the value proposition for the users of Zebi Data Gateway may grow exponentially. The combined value of market available in India for both the products is pegged at \$5 billion⁹ annually.

Zebi is introducing Zebi Coin (ZCO), a utility token which will be used as mode of payment for all Zebi services, including transaction processing through the Gateway and data protection by Zebi Chain™.

Important Notice

PLEASE ENSURE THAT YOU ARE READING THE LATEST VERSION OF THE WHITE PAPER AVAILABLE ON THE WEBSITE OF ZEBI BEFORE YOU MAKE A DECISION TO PARTICIPATE IN THE ZEBI TOKEN SALE. THE LATEST VERSION OF THE WHITE PAPER AMENDS AND REPLACES ANY PRIOR VERSION OF THE WHITE PAPER THAT YOU MAY HAVE REVIEWED.

The Zebi Coin (also referred to as the “**ZCO Tokens**”) when offered and sold are not intended to constitute securities in any jurisdiction. This whitepaper (“**Whitepaper**”) does not constitute a prospectus or offer document and is not intended to constitute an offer of securities or a solicitation for investment in securities in any jurisdiction, and will not be registered under the US Securities Act of 1933 (the “**US Securities Act**”), the Securities and Futures Act (Cap. 289) of Singapore (the “**Singapore SFA**”), or the securities laws of any state, or any other jurisdiction, nor is such registration contemplated. However, out of abundance of caution, ZCO Tokens will be offered and sold in (A) the USA, pursuant to one or more exemptions from the registration requirements of the US Securities Act, namely under Rule 506(c) of Regulation D of the US Securities Act, as amended, and participation in the offering is limited to (i) U.S. “accredited investors” (as defined under a safe harbour for the private offering exemption of Section 4(a)(2) of the US Securities Act as amended and (ii) non-U.S. persons (as defined in Rule 902) in an offshore transaction in reliance on Regulation S of the US Securities Act; and (B) Singapore, pursuant to the exemption(s) provided under Section 302B(1), Section 304, and Section 305 of the Singapore SFA, as amended, and participation in the offering is limited to an “institutional investor” (as defined under Section 4A of the Singapore SFA), a “relevant person” (as defined under Section 305 of the Singapore SFA) or persons to whom an offer is being made (as referred to in Section 305(2) of the Singapore SFA). In all jurisdictions, the offer to sell and solicitation to buy of ZCO Tokens is directed solely to qualified institutional investors, qualified professional investors, and such other sophisticated persons to whom offers and solicitation may be made without any licensing, registration, qualification, or approval under the applicable laws of the relevant jurisdiction (the “Accredited Person”). This Whitepaper does not constitute an offer, distribution, solicitation, or marketing to any non-Accredited Person and is not an offering to the retail public in any jurisdiction where such offering is unlawful.

This Whitepaper is for informational purposes only. The contents of this Whitepaper do not constitute or form part of any opinion on any advice to sell, or any solicitation of any offer to purchase any ZCO Tokens nor shall it or any part of it nor the fact of its presentation form the basis of, or be relied upon in connection with, any contract or investment decision. Prospective purchasers of the ZCO should carefully consider all risks and uncertainties and regulations associated with ZCO, Zebi Blockchain solution and this offering, as set out in this Whitepaper and, more particularly, in the Sections titled “Risks and Uncertainties” and other Sections toward the end of the Whitepaper.

THE RELATIONSHIP BETWEEN ZEBI AND YOU AS A PURCHASER OF ZCO TOKENS IS TO BE GOVERNED ONLY BY A SEPARATE ZEBI UTILITY TOKEN SALE AGREEMENT (“**PURCHASE AGREEMENT**”). IN THE EVENT OF ANY INCONSISTENCIES BETWEEN THE PURCHASE AGREEMENT AND THIS WHITEPAPER, THE FORMER SHALL

PREVAIL. THE PURCHASE AGREEMENT IS A PART OF AND INCORPORATED WITHIN, AND IS TO BE READ ALONG WITH THIS WHITEPAPER.

No regulatory authority has examined or approved of any of the information set out in this Whitepaper. No such action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. This Whitepaper, any part thereof and any copy thereof must not be taken or transmitted to any country where distribution or dissemination of this Whitepaper is prohibited or restricted.

Cautionary Note on Forward-Looking Statements

All statements contained in this Whitepaper, statements made in press releases or in any place accessible by the public and oral statements that may be made by Zebi or its directors, executive officers or employees acting on behalf of Zebi, that are not statements of historical fact, constitute “forward- looking statements”. Some of these statements can be identified by forward-looking terms such as “aim”, “target”, “anticipate”, “believe”, “could”, “estimate”, “expect”, “if”, “intend”, “may”, “plan”, “possible”, “probable”, “project”, “should”, “would”, “will” or other similar terms. However, these terms are not the exclusive means of identifying forward-looking statements. All statements regarding Zebi’s financial position, business strategies, plans and prospects and the future prospects of the industry which Zebi is in are forward-looking statements. These forward-looking statements, including but not limited to statements as to Zebi’s revenue and profitability, prospects, future plans, other expected industry trends and other matters discussed in this Whitepaper regarding Zebi are matters that are not historic facts, but only predictions.

These forward-looking statements involve known and unknown risks, uncertainties and other factors that may cause the actual future results, performance or achievements of Zebi to be materially different from any future results, performance or achievements expected, expressed or implied by such forward-looking statements.

All forward-looking statements made by or attributable to Zebi or persons acting on behalf of Zebi are expressly qualified in their entirety by such factors. Given that risks and uncertainties that may cause the actual future results, performance or achievements of Zebi to be materially different from that expected, expressed or implied by the forward-looking statements in this Whitepaper, undue reliance must not be placed on these statements.

These forward-looking statements are applicable only as of the date of this Whitepaper. Zebi disclaims any responsibility to update any of those forward-looking statements or publicly announce any revisions to those forward-looking statements to reflect future developments, events or circumstances, even if new information becomes available or other events occur in the future.

Market and Industry Information and No Consent of Other Persons

This Whitepaper includes market and industry information and forecasts that have been obtained from internal surveys, reports and studies, where appropriate, as well as market research, publicly available information and industry publications. Such surveys, reports, studies, market research, publicly available information and publications generally state that

the information that they contain has been obtained from sources believed to be reliable, but there can be no assurance as to the accuracy or completeness of such included information.

Save for Zebi and its directors, executive officers and employees, no person has provided his or her consent to the inclusion of his or her name and/or other information attributed or perceived to be attributed to such person in connection therewith in this Whitepaper and no representation, warranty or undertaking is or purported to be provided as to the accuracy or completeness of such information by such person and such persons shall not be obliged to provide any updates on the same.

While Zebi has taken reasonable actions to ensure that the information is extracted accurately and in its proper context, Zebi has not conducted any independent review of the information extracted from third party sources, verified the accuracy or completeness of such information or ascertained the underlying economic assumptions relied upon therein. Consequently, neither Zebi nor its directors, executive officers and employees acting on its behalf makes any representation or warranty as to the accuracy or completeness of such information and shall not be obliged to provide any updates on the same.

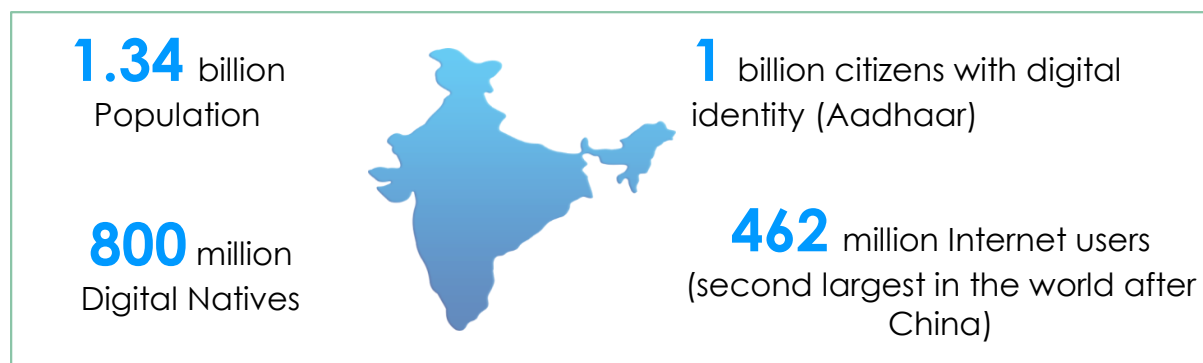
Terms Used

To facilitate a better understanding of the ZCO Tokens being offered for purchase by Zebi, and the businesses and operations of Zebi, certain technical terms and abbreviations, as well as, in certain instances, their descriptions, have been used in this Whitepaper. These descriptions and assigned meanings should not be treated as being definitive of their meanings and may not correspond to standard industry meanings or usage.

Words importing the singular shall, where applicable, include the plural and *vice versa* and words importing the masculine gender shall, where applicable, include the feminine and neuter genders and *vice versa*. References to persons shall include corporations.

The India Opportunity

India is the world's seventh-largest economy and is projected to grow faster than that of any large economy in the world over the next decade. It is at the cusp of explosive growth in technologies such as mobile internet, digital payments, cloud computing and IoT, driven by large number of internet users. As per Ericsson mobility report India's mobile data traffic is expected to increase by 11 times by 2023.



Big Data Boom!!

The Indian economy is witnessing a sea of transformational changes in technology and its adoption. The Government is investing heavily in visionary projects to digitize data and make technology a critical part of the Indian economy. In addition, data generated at an individual level is at an inflection point. India with its burgeoning population of more than a billion, Internet users in excess of 400 million and Smartphone user base of around 300 million is generating massive data⁸.



4G Data wave created with the entrance of low cost telecom carriers enabled the low income Indian population to join the digital bandwagon, allowing a larger chunk of data to be captured, giving a better understanding of customers to businesses and government programs.

Another major driving force is the government's push towards digitization with initiatives like Digital India that aims to transform the country into a digitally empowered society and the National Optical Fiber Network (NOFN) initiative that aims to connect villages with optical fiber and provide high speed internet connectivity. With the entire country planned to be digitally connected, the essential foundations are being laid for phenomenal data generation and consumption over the next decade.

With a median age of 27 years, India is already among the top five, when it comes to active social media and mobile consumers in the world. Big data generated by these fundamental drivers ensure that blockchain powered data protection would establish a booming market, estimated around \$5 billion⁹ annually, providing abundant opportunities to all the stakeholders operating in the ecosystem.

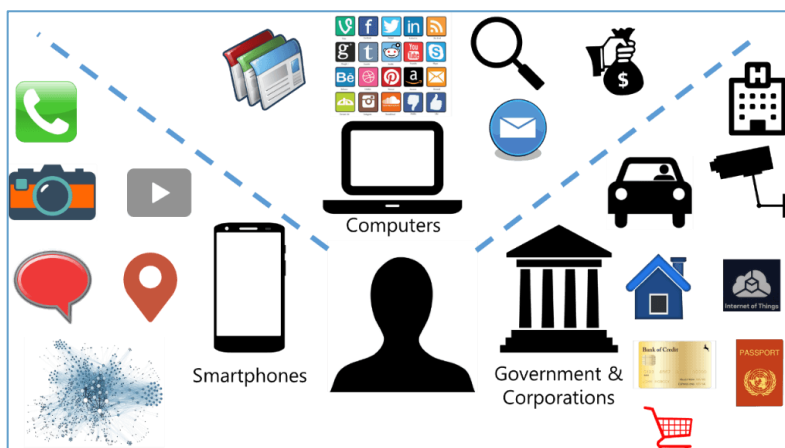
Background

What is happening with Big Data?

According to conservative estimates, India's big data generation is increasing exponentially and is expected to reach 3 Zebibytes per year by 2020¹.

Most of this data is collected and stored by institutions that hold clients' assets centrally such as banks, telecoms, insurance companies, hospitals, governments, and more.

However, in recent years, public media has repeatedly covered controversial incidents related to privacy and security, questioning the



current model, in which centralized organizations collect and control massive amounts of personal data. This model exposes sensitive data to several risks such as:

Data Leaks:

Data leaks happen when private data is exposed to public inadvertently:

- **Reliance Jio (2017) – 120 million customer data leaked¹⁰**
- **Aadhaar (2017) - 210 Government websites made confidential information public¹¹**

Data Tampering:

Data of high value assets like land records are prone to tampering. As land prices continue to rise, scamsters obtain fraudulent documents usually either through "touts" that operate near government offices or by directly bribing the clerks that prepare these documents. As the records are not immutable, such changes cannot be traced with conclusive evidence or certainty.



Another problem with high value information is that majority of Identity and Address proof documents do not have any security marks. With fraudsters using high-precision printers and computers to prepare fake replicas, determining the documents' authenticity by naked eye or physical verification is virtually impossible.

At the same time, the Indian judicial system has some serious inefficiencies burdened by a **thirty million** case backlog, **70%** of which pertain to disputes regarding land or property¹².

Common methods to commit fraud arise from:

- Fake Documents
- Double Mortgages
- GPA (General Power of Attorney)
- Selling Government or Encroached Lands
- Dubious Agreements

Data Hacks:

Another risk of having data stored at one central location is data hacking by malicious hackers from outside the organization. Some prominent examples in the recent past:

- **Zomato data breach is the sixth biggest in 2017**¹³
- **Equifax (2017) – \$4 Billion loss in market cap**¹⁴
- **Yahoo (2017) - \$350 million slashed from valuation in deal with Verizon**

Identities are getting richer, so are data thieves!



At a fundamental level, our identities still include our name, address, credit history, work history and a collection of numbers on our driver's license, Aadhaar card (Govt. Issued ID), PAN card (Income Tax ID), Passport and Employee or Student ID etc. These elements are core to our ability to prove who we are.

However, our identities are getting richer and complex with significant technological innovations such as mobile phones, cloud connected applications and proliferation of devices being connected that touch our everyday lives in novel and innovative ways. The above

infographic shows how data thieves misuse identities.

Identity thefts cost consumers more than \$16 billion

Identity theft is crime of the new millennium. Identity theft is the stealing and use of someone's personal information primarily for monetary gain.

Contrary to popular belief, the primary cause of identity theft is not that more people are online, since these crimes are not limited to online transactions or online banking. Rather it is caused by individuals being careless of sensitive information that they share online or offline, such as personal details, bank or credit card statements, telephone bills, and not guarding sensitive, private information with the care that it deserves.

It is estimated that 19 people fall victim to identity theft, every minute. Identity theft is the largest fraud contributor in *India*¹⁵

Let's check out few instances:

1. Mr. X approached a service provider and was asked to submit his photo ID, address proof and PAN card as KYC (Know Your Customer) documents. Mr. X gave his driver's licence and PAN card in original. This is something all of us do in normal course. The company representative took out multiple photocopies of each of the documents, but submitted only one set to the company, retaining the rest. The representative started using the remaining photocopies for personal use, such as buying a SIM card, etc. Mr. X soon found himself in a big mess as the SIM card was used for illegal activities and the police held him accountable.
2. Ms. Y gave a copy of her phone bill and PAN card as KYC documents to a travel agent for processing visa application. After a few months, she applied for a loan. And her loan application was rejected on the plea that she was a credit card defaulter. She later learnt that the documents were used to obtain credit cards. Several transactions were made, but the amount was never repaid. So, her name appeared on the defaulter's list in the banking records.

As we can see in both the above cases people entered into simple transactions with known service providers and submitted KYC documents like we normally do. However, their personal information in plain text was misused, and they ended up in a sticky situation.

Identity theft can have grave, sometimes devastating repercussions on its victims, ranging from financial loss and damaged credit ratings to the loss of reputation.

Qualification Frauds:

In an increasingly competitive job market, more candidates tend to embellish or fabricate qualifications or experiences on their resume in the hope of securing a highly contested position.

Nearly 10% Indians Lie on Their Resumes to Get Jobs, 50% of them Submit Fake Documents¹⁶

According to a study by Society for Human Resource Management, the cost of a bad hire to an organisation could be up to five times the bad hire's annual salary. There can also be dire consequences such as reputational damage and financial concerns. Besides wrong hires could be a potential risk to the company as they get access to confidential data that they can misuse.

Data Misuse:

Another looming threat to centrally stored data of consumers is misuse of their sensitive information by organizations who have access to it.

- **Airtel Payments Bank License Suspended; Airtel Barred from Conducting Aadhaar-Based E-KYC**¹⁷

What is being done about it? And is it working?

What are Businesses Doing?

With data breaches on the rise, enterprises must constantly develop new strategies and security architecture to safeguard their data assets. Failure to stay in front of data threats will inevitably result in further breaches, financial losses, and tarnished reputations.

Unfortunately, there is no comprehensive enterprise solution to protect customers data from a breach. Organizations typically use traditional solutions such as latest anti-virus software, improved peripherals, network and application level security etc. However, most of these solutions fall short and are unable to provide guaranteed protection against a data breach and subsequent distribution of high value data.

What are Governments Doing?

Consumers are often forced to share increasing amount of personal data to complete a transaction, and once the data is shared they have little or no control over use of their sensitive information.

Banning large-scale data collection is unlikely to be a realistic option to solve the privacy problem. Whether we like it or not, the age of big data has already arrived. We should find the best way of protecting our privacy while allowing legitimate usage of big data, which can make our lives much safer, efficient and more productive.



The present regulatory environment on protection of data is far from ideal. In fact, some countries do not have rules at all. In other cases, the various pieces of legislation introduced are incompatible with each other. Increased reliance on cloud-computing solutions also raise questions about what jurisdictions apply in specific cases. Such lack of clarity creates uncertainty for consumers and businesses, limits the scope for exchange of information and stifles growth.

GDPR enforceable from May 2018, Non-compliance will cost €20 Million+

In a first, the European Parliament adopted the GDPR (General Data Protection Regulation) in April 2016. It carries provisions that require businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. Non-compliance could cost companies steep penalties of up to €20 million or 4 percent of global annual turnover, whichever is higher.

India has set-up expert committee to draft Data Protection Bill

Government of India has set up a committee of experts to study various aspects of data protection and to suggest a data protection bill for India, including data sovereignty.

Will this Help?

Security Solutions or Data Protection Rules alone cannot solve the problem as they still are created and enforced by humans and are prone to be broken.

Blockchain technology and distributed ledgers can provide the solution. Blockchain has already demonstrated trusted, auditable computing in the financial space using a decentralized network of peers accompanied by a public ledger.

Blockchain offers a compelling solution to the problem of combining accessibility with privacy and security, records can be held securely using end-to-end encryption, and yet openly authenticated. Blockchain can enforce privacy and confidentiality rights expected by consumers and regulators while guarding highly sensitive/classified information

What is Needed?

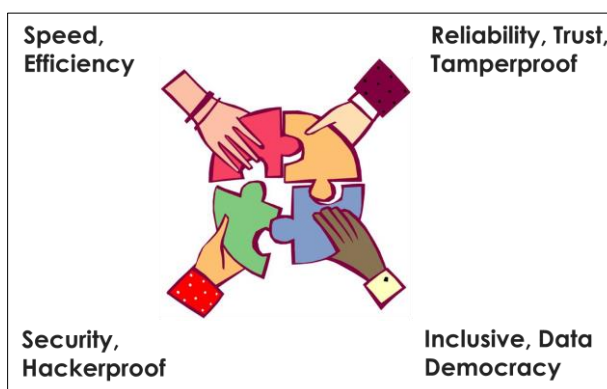
The aggregation of customer data in a single place opens the door for data thieves to make off with all elements of a person's data in one go. This is bound to happen because 100% security is an impossibility. It only requires one security lapse in a data aggregating company like Equifax for the data of hundreds of millions of individuals to be stolen in one go. This is akin to collecting up all your valuables in one "safe" and using a weak lock to secure it. The thief's job is easy now. He does not even need to search the whole house. It gets even worse for data - the valuables are somebody else's, and they don't even know about it.

Need of the hour is a holistic solution which uses Technology to enforce the rules without human intervention and provide:

- Protection from malicious insiders tampering with data
- Security from hackers trying to steal sensitive information
- Mechanism to get consent of individual for every use of their data

None of the systems in the world today can provide a holistic solution of protection of data against tampering by insiders and motivated hackers from outside, and provide a robust mechanism of getting consent for every single use of consumer's data. Zebi team has identified this unmet need and designed a blockchain based solution to tap into this multi-billion-dollar market.

Zebi's Blockchain powered Big Data solution is unique, addressing all of the above challenges and helps to keep data hacker-proof and tamper-proof. It utilizes a distributed ledger on the back-end and a web-app front end, which provides efficient and transparent access to data using DaaS APIs. It will reduce cost of information exchange, remove inefficiencies, enhance security and privacy, and greatly improve fraud detection capabilities for both companies and individuals.



It will bring all the participants in data ecosystem on common platform, thus eliminating manual sharing of personal information, which is prone to misuse.

Zebi Blockchain Solution for Big Data

Introduction

Records have evolved over time, initially we had manual paper based records which were difficult to protect, synchronize and verify because of the manual efforts required, Computers brought automation, but digital records are so easy to copy/manipulate and hence still vulnerable to manipulation. Blockchain technology promises the perfect blend of high availability yet 100% tamperproof especially in case of high value data.

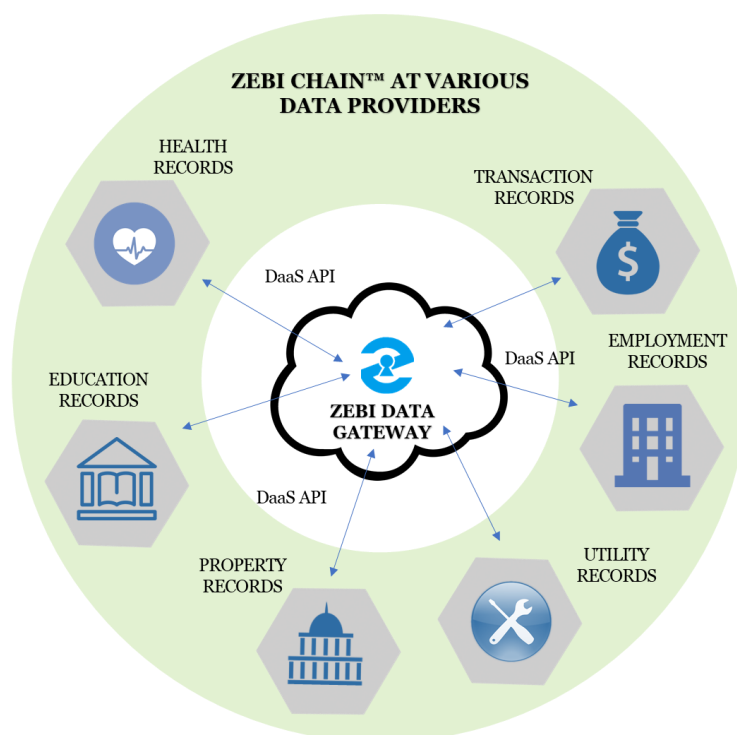
As we have seen so far, the critical aspects when dealing with high value or sensitive data are Immutability, Trusted Verification, Consent, Security, and Privacy. Zebi Blockchain solution will address these aspects while enabling legitimate commercial data sharing activity. Providing complete ownership and control of their data to individuals is at the heart of Zebi solution. Every transaction related to people sensitive data would go through explicit and granular consent mechanism with the convenience of Mobile or Web App.

Bird's-eye view of the solution

Zebi solution ecosystem consists of 2 interconnected proprietary Components *Zebi Chain™* and *Zebi Data Gateway*, to bring

- **Individuals** (Who's data is being protected),
- **Data providers** (Who generate and store their data), and
- **Data Requestors** (Who need to use/validate this data of individual as part of their business process)

on a common platform and enable secure, seamless and consent based exchange of information among them.



Zebi Chain™ is a proprietary light weight satellite application installed at various Data Providers' premises to provide immutability using Blockchain based ledger. The number of nodes in the private Blockchain is configurable and integrates with Ethereum public Blockchain for 100% tamperproof protection.

Zebi Data Gateway connects Zebi Chain™ installations and on-board individuals and data requestors with a simple registration process. It can facilitate instant data exchange through DaaS APIs by connecting to Zebi Chain™ instances and taking individual consent wherever appropriate.

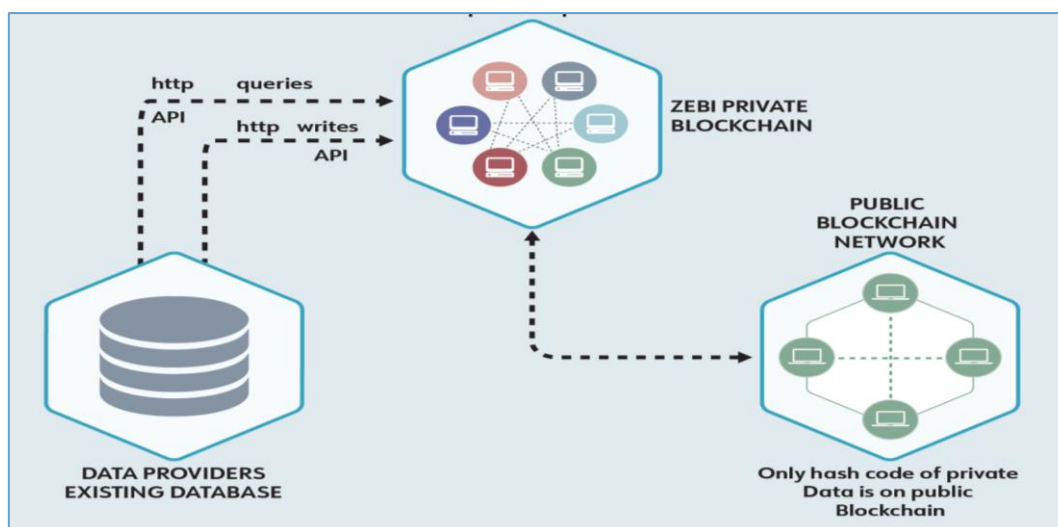
Zebi is starting out with the model of implementing Zebi Chain™ on-premise software at data providers, to connect multiple data sources to Zebi Data Gateway. Zebi Chain™ has already been selected as the solution of choice by one of India's largest state governments to

safeguard their land assets⁶. We see a healthy pipeline of prospects across India. As we scale rapidly and on-board more data providers, the value proposition of Zebi Data Gateway to data requestors increases exponentially.

Let's look at these components in more detail:

Zebi Chain™

Zebi Chain™ is key component of Zebi Blockchain Solution and can be installed on the premises of Data providers such as Universities, Education Boards, Enterprises or Government Departments who generate, issue, update and facilitate data required by data requestors.



It's a very light weight application which can be installed and set-up quickly and has following key features:

- Blockchain based immutability for access and updates on records of documents
- A single node application or a private permissioned blockchain between a group of data owners
- Facilitates seamless DaaS API based data exchange process
- Eliminates need for manual effort required to attend data requests and manual checking of records
- Enables data exchange without any human intervention, hence doesn't leave any scope for manipulation or copying of sensitive information by unscrupulous insiders
- Hash of private data is stored on public blockchain giving superior tamper proof and other benefits such as publishing of hash on 25,000 nodes across the globe and zero downtimes
- All data creation and changes are accompanied with digital signatures of the individual performing such updates on Zebi Chain

Records which will be protected:

- Property Records
- Educational Records
- Employee Records
- Healthcare Records
- High Value Transactions
- Utility Records

Zebi Data Gateway:

Zebi Data Gateway connects with Zebi Chain™ installations done at data providers premises. It allows individuals and data requestors to register with a simple registration process to bring all of them together on a common platform and facilitate secure and seamless data exchange through blockchain powered DaaS APIs.

A registered requestor can submit a data request by filling in relevant details including details of individual and data provider involved, and Zebi Data Gateway shall validate and connect to respective individual to get his/her consent, upon receipt of individuals consent, Zebi Data Gateway shall route the information to respective data provider's Zebi Chain™ application through DaaS APIs, and pass on responses received to Data Requestor instantly. Every part of this process shall be completely automated and hence enables true paperless exchange of information. Moreover, all communications and transactions shall be recorded on immutable blockchain based audit trails.

The Zebi Data Gateway module is a blockchain system driven by Smart Contracts with no human intervention. Though raw data is not saved in Zebi Data Gateway system, following are stored on blockchain for each data access/exchange cycle:

- Who requested for which subject's information when
- When was the subject's consent requested and granted/denied for this data sharing
- What data of the subject was accessed from which data provider.
- Who received/paid what monetization from this data access

Storage on blockchain ensures immutable record of all the above leading to accountability and transparency.

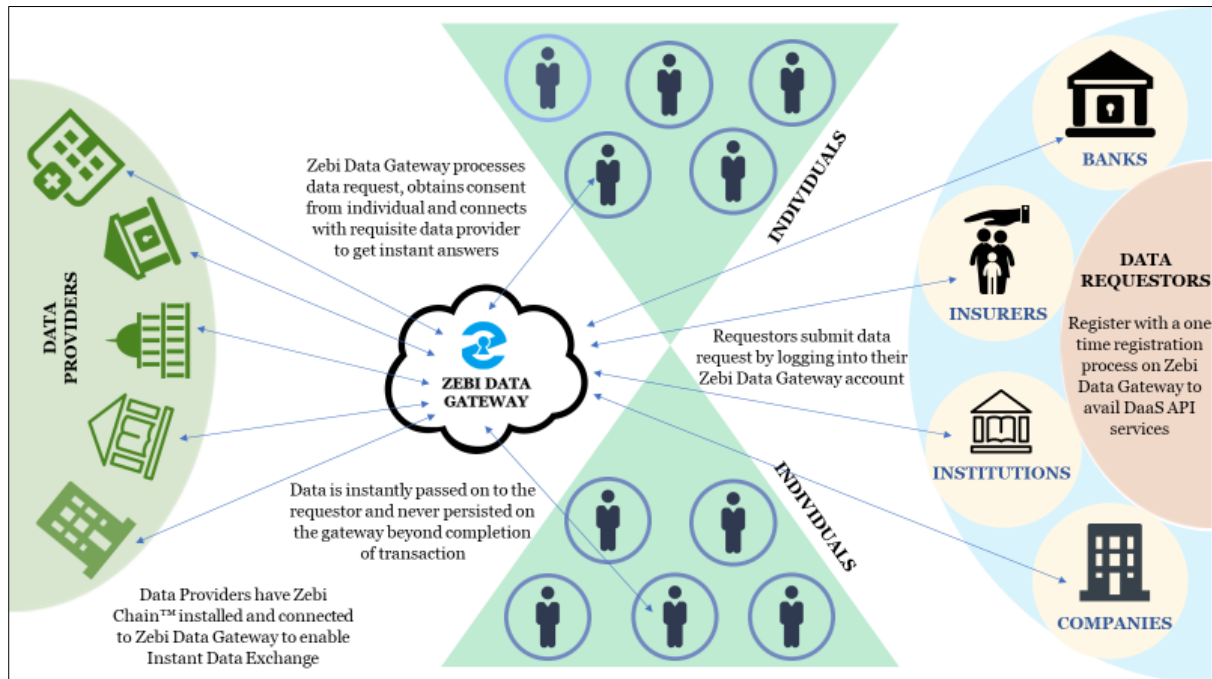
The smart contract also enforces consent based sharing of data and computation of the money earned owed by each player across the cycle and transfers Zebi Coin tokens across respective accounts as part of the same cycle

Smart contracts ensure that data exchange occurs only with consent and that all stake holder receive their deserved share of the data monetization.

How Zebi Data Ecosystem will transform Industries

Industries which will be transformed with scope for complete business automation:

- Protection and Verification of Land Registry and other high value records
- Consumer Lending
- Credit Scoring
- Direct Marketing
- Corporate Recruitment



Zebi Data Ecosystem will transform the way records are maintained by data providers and used by requestors (for verifying information), while keeping individuals in loop for every use of their data. It will open whole new set of possibilities which the current day systems are not able to provide, enhancing utility for its users.

FOR DATA PROVIDERS:

- It will help to keep their data secured from hackers and malicious insiders who can manipulate with it
- Make it available for instant DaaS API based applications through Zebi Data Gateway, with assured share in revenues from the requestors for the same.
- Enable consent mechanism before sharing individual's data for a data exchange transaction
- Reduce time and efforts to attend to a data request vis-à-vis the current paper based and manual process
- Improve revenues from verification requests as due to instant data exchange the volume of transactions will increase exponentially as more and more businesses will be able to adopt it

FOR DATA REQUESTORS:

- It will cut down on time, efforts and costs of verifying data directly from source
- Due to instant data exchange, it will become feasible for every record to be verified, which was not practical earlier due to lengthy process, and was often overlooked
- Improve recruitment effectiveness and preventing exorbitant costs of a bad hire
- DaaS API's can be integrated with their applications to automate the verification process completely

FOR INDIVIDUALS:

- Improved protection from identity thefts, fake documents and monetary losses due to theft of their sensitive information

- Unlike existing systems which do not have notification to individuals, in Zebi Data Ecosystem individuals will be notified first before their information is shared/used by anyone

Let's see a couple of examples of how some industries will get transformed by Zebi Data Eco-system:

Home Loan Processing:



- Individual applies loan with bank and submits bundle of photocopies of property link documents for the same
- Bank reviews all the documents manually and gets the property documents verified by having agents visit to registrar office several times
- Registrar must search and print all the relevant information manually from the records
- Verification process takes few weeks and so loan disbursement process takes more than a month
- With limited resources the banks capacity to process loans is limited

- Individual applies for loan with bank and must submit only blockchain asset certificate from registrar
- Bank reviews all the details and logs it into ERP for processing
- ERP automatically calls DaaS API to Zebi Data Gateway to verify the ownership of property
- Verification happens instantly, with owner's consent and the loan disbursement can happen within day or two
- As entire process is accelerated by instant data exchange, more number of applications can be processed with the same resources.

Credit Scoring:



- Banks generate weekly or fortnightly dumps of consumers accounts to share with credit rating agency
- Credit agency gets dumps from various banks and update their records periodically
- On receipt of Credit Score request, they need to search and check the availability of up to date data
- Credit rating agency must contact relevant bank to request updated information of account, which takes couple of days
- On receipt of relevant data its consolidated to provide credit score of the individual

- On receipt of credit score request credit rating agency can initiate DaaS API call through Zebi Data Gateway for up to date statements instantly
- Apart from Banking transactions, other relevant information such as high value transactions, utility payments history etc. can also be used for more comprehensive credit score
- More requests can be processed as instant data exchange through Zebi Data Gateway can be integrated into their application for faster processing
- Everything happens with prior consent of the individual

Qualification Check:

Before
& After

- Candidate submits his qualification certificate soft copies to prospective employer
- Employer initiates qualification check process through background check agency, by sharing soft copies of certificates
- Agency personnel visits university or board to submit verification request manually which takes few days
- Agency personnel collects verification report from university in due course and reverts to client with confirmation
- Entire process is manual, email based and takes up to 2 weeks, with no notification to individual

Candidate submits his qualification certificate copies to prospective employer

- Employer submits data request through Zebi Data Gateway
- Zebi data gateway connects to individual for his/her consent
- Zebi data gateway connects to Zebi Chain application of respective University and gets instant validation of the data, which is instantly shared with the Employer
- As this entire process takes just few minutes and can also be integrated into company's system, it's possible to perform check on bulk of candidates during a recruitment drive

Revenue Model

Zebi Chain™ is being offered as an on-premise software in either License + Annual Maintenance Cost (AMC) mode or monthly subscription mode, depending on the comfort and choice of the Data Provider. Zebi Data Gateway shall charge transaction fees for every transaction made through it from the Data Requestors. The revenue from Data Requestors is shared with Data Providers and Individuals as an incentive to enable seamless transaction processing. Zebi will add more features to its products such as enabling blockchain secured seamless payments (FIAT as well as Crypto currencies) for all the transactions processed on its Blockchain solution.



License/
Subscription
Revenues



Recurring Support
Revenues and
Transaction Fees



DaaS API
Revenues

Status of Product and Market Development



Completed So Far

- Solution with basic features ready
- ISO 27001 Information Security certified
- One patent filed in India
- A multi-year subscription work order for Zebi Chain™ signed with Andhra Pradesh (10th largest state with population of over 50 million people) and billing initiated



Pursuits in Progress

- Two patents in progress
- Passed technical evaluation and awaiting results of financial evaluation from AP and Telangana governments
- Submitted proposals to governments and enterprises across India, Singapore, the United States and other countries

Road Ahead

Year	Qtr.	Details
2018	Q1	Promote Zebi Chain for Land Registry and Property records to other government agencies
		Promote Zebi Chain for Educational records
	Q2	Zebi Chain for Employment records
		Integration with Ethereum
	Q3	256 bit encryption enabled on Zebi platform
		APIs for authentication, verification and consent mgmt.
	Q4	Data cleansing and mgmt. with AI/ML/DL
		Simple (1X1) Smart Contracts and transaction processing through Zebi Chain platform
2019	Q1	DaaS APIs for Data Owners/Requestors/Providers
	Q2	Zebi Pay launched
		Integrated with leading blockchain payment gateways
	Q3	Seamless end-to-end transaction processing
		Crypto/FIAT currency capable
Q4	Zebi Verify launched for Education/Employment verticals	
2020	Q1	Zebi Insights launched
	Q2	Algorithms and APIs for Data/Insights sharing using Smart Contracts
	Q3	Compounded (nXn) Smart Contracts
	Q4	Promote Zebi Insights/Smart contracts to enterprises

Zebi Coin (ZCO) Sale

Zebi Coin:



Zebi Intends to introduce **Zebi Coin (ZCO)**, which will be utility token to be used as incentive for settlement of transactions within the Ecosystem. The ZCO paid by Requestor for a data transaction will be distributed among Data Provider, Individual and Zebi as a reward for making the transaction happen. The proportion in which this sharing will happen will be governed by a smart contract which can be adjusted by consensus among the participants. ZCO will incentivize all participants to use, contribute and grow the Zebi Data Ecosystem. Thus ZCO will be the fourth member of the Ecosystem which will keep all the members bonded with each other in their collective growth journey.

Token Sale Model:

Maximum Cap: Overall US \$10 Million

Presale: \$2 Million

Crowdsale: \$8 Million

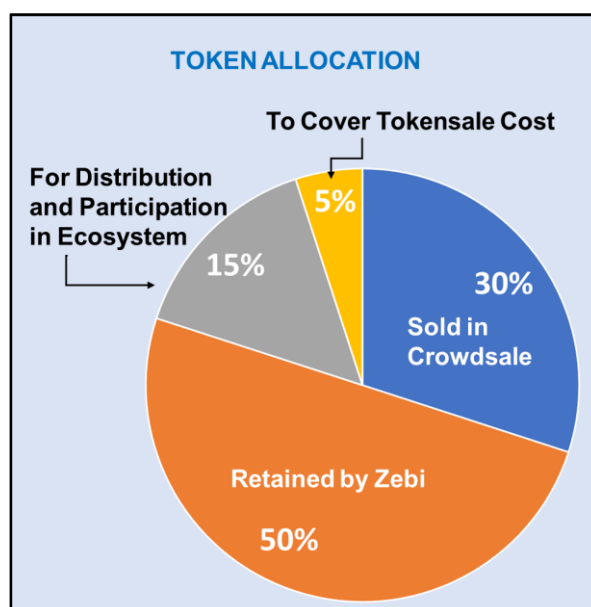
(Pegged at 1 ETH = \$1,000)

Token Name: Zebi Coin (ZCO)

Standard: Ethereum ERC20

Total Token Supply: 1 Billion ZCO's of which:

- **300,000,000** to be sold in the token sale
- **500,000,000** to be retained by Zebi as company reserves for allocation to founders, team, advisors, data providers and other partners and released for purchase from time to time depending on demand. Maximum of 35% (175,000,000) will be allocated to founders, team, and advisors
- **150,000,000** to be allocated distribution and participation in ecosystem (including for bounties)
- **50,000,000** To cover the token sale costs



Note:

- Company reserves are locked up for a period of 18 calendar months commencing from March 2018 and may be released in phases only after the completion of the aforementioned 18 months' period. Further, no more than 12.5% of the total tokens issued by Zebi pursuant to the ZCO token sale may be transferred/ released by Zebi, from its holdings, in any calendar year.
- Anything remaining from the aforementioned allocations shall be moved into company reserves.

Sale of tokens shall be limited to ensure that token holders can be serviced appropriately and are able to derive maximum utility from the Zebi Blockchain Solutions.

Purchase of Tokens:

Token Price: 1 ZCO = 0.0000333 ETH

Minimum Purchase: 3000 ZCOs or 0.1 ETH

Key Dates:

Pre-Sale Announcement Release Date: 05-Feb-2018

Pre-Sale End Date: 12-Feb-2018

Token Sale Release Date: 05-Mar-2018

Token Sale End Date: 31-Mar-2018

Resale/Exchange Trading of ZCO's: April 2018

Bonuses:

Presale:

30%

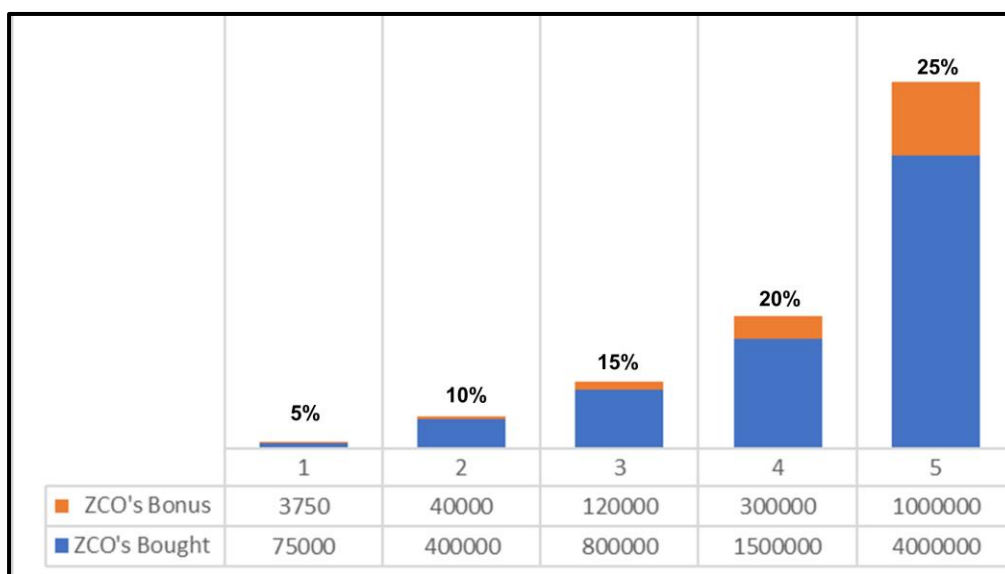
Crowdsale:

Early Bird Bonus:

10% for First 48 hours

Volume Bonus:

ZCO's Bought	Bonus %	Bonus ZCO's
75,000	5%	3,750
400,000	10%	40,000
800,000	15%	120,000
1,500,000	20%	300,000
4,000,000	25%	1,000,000



Note: For enquiring about purchases above 4,000,000 ZCOs, kindly write to us at info@zebi.co.

Additional Notes:

Future Product Development:

1. Data Issuer Basic Issuers who will have just light weight App to respond to Zebi APIs
2. Data Issuer Premium App which would have dedicated private blockchain implementation at Issuer's end.
3. Zebi App for Individuals which would facilitate registration, distribution of private keys and consent mechanism for data requests.

Operations and Marketing:

- Acquiring, engaging and servicing the prospective Individuals, Issuers & Requestors to enhance utility of the Zebi Data Ecosystem.
- Expanding teams required for functioning of Operations, Sales and Engineering
- Engaging technical and strategy advisors to ensure Zebi stays on right course
- Incentivizing Ecosystem participants to encourage them to contribute towards adoption and growth of Zebi Data Eco-system

Resale/Exchange/Buy-back of ZCO:

Subject to risks highlighted in the Section titled "Risks and Uncertainties", beginning April 2018, holders of the ZCO shall be able to sell their ZCO to interested purchasers, if they are unable to or don't intend to derive utility from the ZCO. ZCO holders may be able to exchange their ZCO for other cryptocurrencies or fiat currencies, depending upon applicable laws and market conditions. From time to time, Zebi may use some of its profits to buy back limited quantities of ZCO's from holders, to enable them to exit their holdings if they are unable to derive utility from the ZCO.

Team



BABU MUNAGALA

Founder, CEO & Managing Director
20+ Years of Silicon Valley Experience
B. Tech, IIT Madras, ME, Indian Institute of Science (IISc);
MS, Ohio State University



SUDHEER KUPPAM

Co-Founder and Board Member,
Managing Partner, Epsilon Venture Partners
18+ years in VC industry in Silicon Valley and Asia Pacific
B. Tech, IIT Madras; MS, Rensselaer Polytechnic Institute



KALYAN MUPPANENI

Board Member,
Founder, MD & CEO of Pi Datacenters,
Prev. Enterprise Architect at Intel
Corporation



PHANI AREGA

Vice President, Engineering
20+ yrs. of IT Experience
B.Tech, IIT Madras



GOPAL BANG

Director, Business Operations
13+ yrs. of Operations Experience
MBA, ICWAI, EPBA



RENUKA RATHODE

Product Strategist
4 yrs. of Product Development Experience
IIITDM

Advisors



VASU PARMESWARAN

Stealth Mode AI/ML Start-up; Ex Uber, Ex Microsoft, Ex Nokia; Ph.D. Computer Science, M.S. Computer Science, M.S. Aerospace Engineering, University of Maryland College Park; B. Tech. IIT Madras.



PHIL MUI

SVP Technology, Salesforce
Ex Axiom, Ex Google; PhD, M.Eng MIT; M.Phil Oxford University; Management, Stanford University;



NARENDRA GOGULA

Managing Director IT Services Co.
Ex Infosys; B.Tech, IIT Madras.



SRIDHAR GADHI

Founder & CEO at Quantela Inc. Ex IBM, Ex Tech Mahindra; Harvard Business School



RAJU INDUKURI

Serial Entrepreneur; Honorary Chairman, Andhra Pradesh Global Network; Co-Founder & Executive Chairman, Quantela Inc; M.S, University of Illinois Springfield



PRAHALAD THOTA

SVP & Head of Enterprise Analytics and Data Science, Wells Fargo; Ex- Charles Schwab, Ex- PayPal; M.S. Finance, Virginia Tech; MBA, IIM Bangalore; M.S., Aerospace Engineering, Georgia Institute of Technology; B.Tech, IIT Madras



TG GANESHAN

VP Finance, Equian Healthcare Technology company
Ex- Hilton Worldwide, Ex- SeaWorld Parks & Entertainment; MBA, University of Texas at Austin; M.S, Auburn University; B.Tech, IIT Madras



CHANDRA MALLIPEDI

Principal Engineer, Predictive Analytics
Ex-Amazon, M.S, B.S, Material Engineering, Auburn University; B.Tech, IIT Madras



BHAVESH SHAH

Consultant - Digital Marketing & Analytics, ex Kaiser Permanente, ex-Capital One, ex-Bombay Stock Exchange. BE, University of Mumbai; MBA, XLRI Jamshedpur



BHASKER ALLAM

Software Engineer, Stealth Security, Inc.
Ex-RSA, Ex-Juniper; MS, Computer Engineering, Old Dominion University; B. Tech., ECE JNTU



ANIRUDH RASTOGI

Managing Partner TRA; BA. LLB. (Hons)., National Law Institute University, LL.M. (Master of Laws), Harvard Law School



RAO SURAPANENI

Senior Director, ServiceNow; Ex-Microsoft, Tellme Networks, Veraz Networks, Lucent, AT&T Bell Labs; MBA - UC Berkeley-Haas School of Business, MS in CS - University of Kentucky, B.Tech in CS - NIT Warangal

Additional Terms and Conditions

Disclaimer Of Liability

To the maximum extent permitted by the applicable laws, regulations and rules, Zebi shall not be liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising out of or in connection with any acceptance of or reliance on this Whitepaper or any part thereof by you.

No Representations and Warranties

Zebi does not make or purport to make, and hereby disclaims, any representation, warranty or undertaking in any form whatsoever to any entity or person, except as specifically set forth under this Whitepaper.

Representations and Warranties by You

This Whitepaper is solely for your information and may not be reproduced, disclosed or distributed to any other person, unless authorized by us. By accessing and/or accepting possession of any information in this Whitepaper or such part thereof (as the case may be), or acting on it, you represent and warrant to Zebi and agree to be bound by the disclaimers, limitations and restrictions described herein, and in addition to the following:

- (a) you agree and acknowledge that the ZCO Tokens do not constitute securities in any form in the jurisdiction of which you are a citizen, resident (tax or otherwise) or green card holder;
- (b) you agree and acknowledge that this Whitepaper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities or a solicitation for investment in securities which is registered with the appropriate regulatory authorities in the jurisdiction of which you are a citizen, resident (tax or otherwise) or green card holder.
- (c) you agree and acknowledge that no regulatory authority has examined or approved of the information set out in this Whitepaper, no action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction and the publication, distribution or dissemination of this Whitepaper to you does not imply that the applicable laws, regulatory requirements or rules of the jurisdiction of which you are a citizen, resident (tax or otherwise) or green card holder have been complied with.
- (d) the distribution or dissemination of this Whitepaper, any part thereof or any copy thereof, or acceptance of the same by you, is not prohibited or restricted by the applicable laws, regulations or rules in your jurisdiction, and where any restrictions in relation to possession are applicable, you have observed and complied with all such restrictions at your own expense and without liability to Zebi;
- (e) you agree and acknowledge that in the case where you wish to purchase any ZCO Tokens, the ZCO Tokens are not to be construed, interpreted, classified or treated as:
 - (i) any kind of currency other than cryptocurrency;
 - (ii) debentures, stocks or shares issued by any person or entity
 - (iii) rights, options or derivatives in respect of such debentures, stocks or shares;

- (iv) units in a collective investment scheme;
- (v) derivatives of units in a business trust; or
- (vi) units in a business trust;
- (vii) any other security or class of securities.

(f) you have a basic degree of understanding of the operation, functionality, usage, storage, transmission mechanisms and other material characteristics of cryptocurrencies, blockchain-based software systems, cryptocurrency wallets or other related token storage mechanisms, blockchain technology and smart contract technology;

(g) you are fully aware and understand that in the case where you wish to purchase any ZCO Tokens, there are risks associated with Zebi and its business and operations, the ZCO Tokens, the Zebi Token Sale (each as referred to in the Whitepaper);

(h) you agree and acknowledge that neither Zebi is liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising out of or in connection with any acceptance of or reliance on this Whitepaper or any part thereof by you; and rights under a contract for differences or under any other contract the purpose or pretended purpose of which is to secure a profit or avoid a loss;

(i) You are competent to contract i.e. in case of individuals, you are over eighteen (18) years of age, and in case of legal entities, you are duly authorized by such legal entity to act on its behalf.

(j) You are a U.S. “accredited investor” (as defined under the US Securities Act, Rule 501 of regulation D).

(k) all of the above representations and warranties are true, complete, accurate and non-misleading from the time of your access to and/or acceptance of possession this Whitepaper or such part thereof (as the case may be).

No Advice

No information in this Whitepaper should be considered or construed to be business, legal, financial or tax advice regarding Zebi, the ZCO Tokens and the Zebi Token Sale (each as referred to in the Whitepaper). You should consult your own legal, financial, tax or other professional adviser regarding Zebi and its businesses and operations, the ZCO Tokens, and the Zebi Token Sale (each as referred to in the Whitepaper). You should be aware that you may be required to bear the financial risk of any purchase of ZCO Tokens for an indefinite period of time.

No Further Information or Update

No person has been or is authorised to give any information or representation not contained in this Whitepaper in connection with Zebi and its business and operations, the ZCO Tokens, and the Zebi Token Sale (each as referred to in the Whitepaper) and, if given, such information

or representation must not be relied upon as having been authorised by or on behalf of Zebi. The Zebi Token Sale (as referred to in the Whitepaper) shall not, under any circumstances, constitute a continuing representation or create any suggestion or implication that there has been no change, or development reasonably likely to involve a material change in the affairs, conditions and prospects of Zebi or in any statement of fact or information contained in this Whitepaper since the date hereof.

Restrictions on Distribution and Dissemination

The distribution or dissemination of this Whitepaper or any part thereof may be prohibited or restricted by the laws, regulatory requirements and rules of any jurisdiction. In the case where any restriction applies, you are to inform yourself about, and to observe, any restrictions which are applicable to your possession of this Whitepaper or such part thereof (as the case may be) at your own expense and without liability to Zebi.

Persons to whom a copy of this Whitepaper has been privately distributed or disseminated, provided access to or who otherwise have the Whitepaper in their possession shall not circulate it to any other persons, reproduce or otherwise distribute this Whitepaper or any information contained herein for any purpose whatsoever nor permit or cause the same to occur.

Data Privacy and Security

Zebi is committed to ensuring that your data is secure. In order to prevent unauthorized access or disclosure, Zebi has put in place suitable physical, electronic, and managerial procedures to safeguard and secure your data.

All the data provided to us is stored in a secure computing environment protected by secure firewalls to prevent unauthorized access. The company controls access so that only people who need to access the purchaser data are granted access. All team members of Zebi are provided security training and are required to adhere to a comprehensive set of security policies, procedures, and standards related to their jobs.

When you use secure areas of the Zebi website, Secure Sockets Layer (SSL) protocol is used with 128-bit encryption. This means that all the information sent between your computers and the Zebi secure computer environment is encrypted so that it cannot be read in transit. Secure areas of the site have a time-out feature. If you leave a secure session inactive for some time, the site times-out to prevent unauthorized access.

It is possible that Zebi may be required by law, court order, or other legal process to provide information about our customers to outside parties, including for compliance purposes for regimes, such as the General Data Protection Regulation and the (Indian) Information Technology Act, 2000. It is the company's policy to ensure adherence to the due process of law in all such instances, and if required to provide information under these circumstances, the company will, whenever possible, attempt to inform users whose information has been requested, unless prohibited by law.

Zebi may also retain copies of personal information to comply with legal obligations, pursuant to the company's data retention policies, or for such reasonable period as is required to address potential disputes.

Zebi has developed privacy policies and practices that strive to protect the privacy rights of its users.

Country Specific Disclaimers and Restrictions

The ZCO Tokens are not intended to constitute securities in any jurisdiction. However, in the event a securities regulator were to take a contrary view that the ZCO Tokens constitute securities, this offering is also intended to qualify for exemption from registration in certain jurisdictions where this offer may be made:

United States of America

In the event this Whitepaper is being furnished to you in the United States of America (including Puerto Rico and the U.S. Virgin Islands), it is being furnished on a confidential basis and solely for your information and may not be reproduced, disclosed or distributed to any other person. You acknowledge and agree that the offer of ZCO Tokens in the United States is being made pursuant to Rule 506(c) of Regulation D of the US Securities Act, as amended and participation in the offering is limited to (i) U.S. “accredited investors” (as defined under the US Securities Act, Rule 501 of regulation D) considered “a safe harbour” for the private offering exemption of Section 4(a)(2) of the US Securities Act as amended and (ii) non-“U.S. persons” (as defined in Rule 902) in an offshore transaction in reliance on Regulation S of the US Securities Act. Further, you agree to be bound by the disclaimers, limitations and restrictions described under regulation D of the US Securities Act.

Singapore

In the event this Whitepaper is being furnished to you in Singapore, it is being furnished on a confidential basis and solely for your information and may not be reproduced, disclosed or distributed to any other person. By accepting this document, you (i) represent and warrant that you are either an “institutional investor” (as defined under Section 4A of the Singapore SFA), a “relevant person” (as defined under Section 305 of the SFA), or persons to whom an offer is being made (as referred to in Section 305(2) of the SFA); and (ii) agree to be bound by the disclaimers, limitations and restrictions described herein.

The purchaser acknowledges that the offer of interests herein is made in reliance on the exemption(s) provided under Section 302B(1), Section 304, and Section 305 of the Singapore Securities and Futures Act (Cap. 289) (“SFA”) and is not made in or accompanied by a prospectus that is registered by the Monetary Authority of Singapore and pursuant thereto the purchaser further acknowledges and unconditionally undertakes that the interests offered herein and accepted by the purchaser in accordance with the terms and condition herein shall not be subsequently sold to any person, unless the offer resulting in such subsequent sale is made in compliance with the SFA and/or in reliance on any applicable exemption(s) provided

under the SFA.

Risks and Uncertainties

Project Risks

Prospective purchasers of ZCO (as referred to in this Whitepaper) should carefully consider and evaluate all risks and uncertainties associated with Zebi, the Zebi Blockchain Solution, the ZebiCoin and the Zebi Token Sale (each as referred to in the Whitepaper), all information set out in this Whitepaper and the Purchase Agreement prior to any purchase of ZCO. If any of such risks and uncertainties develops into actual events, the inherent utility of the Zebi Blockchain Solution and the ZCO could be materially and adversely affected.

Below are some illustrative risks associated with this Zebi Token Sale. This list is not meant to be exhaustive as the market and regulatory environment are quickly evolving.

Zebi Blockchain Solution Utility Risks

Security Risk

If our security measures are breached, or unauthorized access to data of our clients or their employees is otherwise obtained, our solution may not be perceived as being secure, clients may reduce the use of or stop using our solution adversely affecting the utility of the Zebi Blockchain solution.

Our solution involves the collection, storage and transmission of clients' and their employees' confidential and proprietary information, including personal or identifying information, as well as financial and payroll data. Unauthorized access or security breaches could result in the loss of information and utility, litigation, indemnity obligations and other liability.

Blockchain-based DaaS Market

If the Blockchain-based DaaS market develops more slowly than we expect or declines, our utility may slow or stall, and the Zebi Blockchain Solution could be adversely affected.

The Blockchain-based DaaS market is not as mature as the market for on-premise enterprise software, and it is uncertain whether Blockchain-based DaaS will achieve and sustain high levels of demand and market acceptance.

Blockchain-based solution volatility

Real or perceived errors, failures, or disruptions in the Zebi products and solutions could adversely affect our customers' satisfaction with our solutions and/or our industry reputation and The Zebi Blockchain solution utility could be harmed.

The Zebi products and solutions are very complex and have contained and may contain undetected defects or errors. The Zebi products and solutions are often used in connection with large-scale computing environments with different operating systems, system management software, equipment and networking configurations, which may cause errors or failures of products, or other aspects of the computing environment into which our products are deployed

ZCO

Absence of Rights

ZCO does not grant any rights, explicit or implied, in Zebi. ZCO is not a tool for owning any assets of Zebi.

Refund or Resale

Zebi is not obliged to redeem ZCO, or to otherwise refund their holders, for whatever reason. ZCO's value upon resale is not and will not be guaranteed, including their inherent value. *Aside from that, a resale may be limited by laws and regulations that differ from the laws and regulations applicable to the ZCO holder.* The resale market for ZCO may not be active.

Blockchain and Software

Processing of Smart Contracts

In the Bitcoin and Ethereum blockchains, block production can occur at arbitrary times, so there is a risk of untimely performance of smart contracts. The holder should be aware of this and consider its probability. The Bitcoin or Ethereum blockchains may not process a transaction at the exact moment the buyer expects it, and the buyer might not receive ZCO on the same day that it completes the necessary action.

Network Overload

The Bitcoin and Ethereum networks are subject to congestion, when transactions can be lost or delayed. Individuals and groups can deliberately congest entire networks, trying to gain an advantage.

Functionality

The Zebi Blockchain Solution may become obsolete or lose relevance due to the fast pace of innovations.

Security

Lost Private Keys

ZCO may be stored in a digital wallet or other storage requiring a digital key (or combination of keys). The loss of keys associated with a digital wallet or storage, will result in the loss of access to their balances. Additionally, a third party may get access to the private keys from the holder's wallet or storage, and, consequently, access to the ZCO Tokens they contain. Zebi is not liable for the losses that this may entail.

Zebi Infrastructure Security

Hackers or other bad actors may try to intervene in a smart contract, or otherwise interfere with aspects of how Zebi functions. These may include malware attacks, denial-of-service attacks, and other digital disruptions.

Connection of Open Cryptographic Keys

In the event that the ZCO holder does not provide access to connect open cryptographic keys to their account, it may cause a third party to incorrectly recognize the holder's ZCO balance in the Ethereum blockchain, while initial balances of a new Zebi blockchain are formed.

Cryptocurrency Wallet Incompatibility

A wallet or cryptocurrency storage system used by the holder must be technically compatible with ZCO. Failure to use a compatible technology may result in the ZCO holder not gaining access to their ZCO.

Zebi Development

Third-Party Dependency

In the event that Zebi works with multiple third parties, Zebi exerts no control over the actions of the third parties themselves. The utility of the Zebi Blockchain solution may be severely hampered if there is a failure on the part of the third parties in performing the tasks agreed upon. There is no guarantee that these third parties will do their job properly.

Development Team Dependency

This project exists as the result of effort by the Zebi team, who are responsible for maintaining the competitiveness of the ecosystem overall. To lose members of the management team (or to fail to attract and retain additional staff) could have a significant adverse impact on Zebi and the Zebi Blockchain solution. The competition for staff with relevant experience is high due to the small number of qualified specialists. This shortage of personnel seriously affects the ability to attract additional qualified management, which may have a significant negative impact on the Zebi Blockchain solution.

Interest in the Zebi Blockchain solution

The success of the Zebi Blockchain solution depends on the continued interest and participation of third parties. Their interest cannot be guaranteed.

Third-Party Projects

The Zebi Blockchain solution can prompt creation of alternative projects promoted by non-affiliated third parties.

Zebi's Activities

Conflict of Interest

Zebi's units may be involved in transactions with affiliated entities. Conflicts of interest may arise within Zebi or between Zebi and affiliated parties. Transactions with related parties may fail to comply with the arm's length principle.

Emerging Markets

Zebi (or its units) can operate in the emerging markets countries subject to high risks, including significant legal, economic and political risks.

Government

Immature Regulatory Framework

Developments in regulations around the world may alter the nature of our utility or restrict the use of blockchain assets or the operation of a blockchain network upon which we rely in a

manner that adversely affects the Zebi Blockchain solution's utility

As blockchain networks and blockchain assets have grown in popularity and in market size, federal, state and international agencies have begun to take an interest in, and in some cases, regulate their use and operation. In the case of virtual currencies, regulators have created new frameworks or have published guidance as to how existing regulatory frameworks apply to virtual currencies.

Regulators globally, including, but not limited to, Canada, China, Australia, Brazil, India, Singapore, and South Korea, have issued some form of guidance regarding their position on initial coin offerings and token sales. Our utility and the use of ZCO could be adversely affected by depending on whether and how a given regulatory agency decides to exert authority over a blockchain network.

Zebi may stop distributing coins, developing the Zebi Blockchain solution, or its activities in a specific jurisdiction in the event that such actions are found to be illegal, or legislative changes make them economically impractical.

Licenses and Permissions

Although, as of the date hereof, there are no statutory requirements for Zebi or ZCO holders to obtain any licenses or permissions for operations with digital assets, there is a risk that such requirements will be introduced in the future. Regulatory authorities may establish requirements for cryptocurrency traders, including requirements for compliance with various standards, getting licenses, identification, reporting, and the like. In this case, an exchange trading in ZCO could be suspended for an indefinite period.

State Regulation

Zebi operates in a new industry and may be subject to increased supervision and control. Withdrawal or amendment of regulatory authorizations with respect to all or part of the activities carried on by Zebi or with respect to the fitness and propriety of one or more individuals to perform their current roles (including any of the Directors) might oblige Zebi to cease conducting a particular type of activity, or modify the manner in which it is conducted.

Zebi's property and operations are regulated by various public authorities and are subject to annual inspections. An inspection may conclude that Zebi has violated laws, decrees, or regulations, and cannot refute these findings or rectify the violations in a timely manner.

The failure by Zebi to obtain prior regulatory authorization in a jurisdiction where it has operated or the refusal of a regulator to grant that authorization in a jurisdiction where it may wish to operate could prevent Zebi from maintaining or expanding the Zebi Blockchain solution. Failure to comply with the applicable laws or orders resulting from the inspections can lead to significant penalties, ranging from fines to administrative or criminal prosecution of Zebi's officials.

Actions of Public Authorities

Sometimes public authorities show a high degree of freedom. Under the influence of commercial or political considerations, they act selectively, arbitrarily, without prior notice, or in a manner contrary to the law. This creates risks for Zebi's operations. Furthermore, such

conditions allow competitors to gain various privileges and preferences from public authorities, equating to direct competitive advantages.

Privacy Concerns

Privacy concerns and laws or other domestic regulations may drive the adoption of the ZEBI Blockchain solution but at the same time may reduce its effectiveness. Our applications require the storage and transmission of the proprietary and confidential information of our clients and their clients, including personal or identifying information, as well as their financial and payroll data.

A wide variety of domestic and foreign laws and regulations apply to the collection, use, retention, protection, disclosure, transfer, disposal and other processing of personal data. These data protection and privacy-related laws and regulations are evolving and may result in regulatory and public scrutiny and escalating levels of enforcement and sanctions. In India, there exists no formal data protection laws and is currently governed by specific sections (43A, 65, 69 and 72A) under The (Indian) Information Technology Act, 2000. The regulations surrounding data protection is bound to change with the impending Data Privacy Act to be implemented by the Indian government in the months to come.

In addition to government regulation, privacy advocates and industry groups may propose new and different self-regulatory standards. Because the interpretation and application of privacy and data protection laws are still uncertain, it is possible that these laws may be interpreted and applied in a manner that is inconsistent with our existing data management practices or the features of our solution.

All of these legislative and regulatory initiatives may adversely affect the ability of our clients to process, handle, store, use and transmit demographic and personal information from their employees, which could reduce demand for our applications.

IF YOU ARE IN ANY DOUBT AS TO THE ACTION YOU SHOULD TAKE, YOU SHOULD CONSULT YOUR LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S).

References

1. <http://www.thehindubusinessline.com/info-tech/digital-data-generated-by-india-in-2012-equals-mt-everest/article4435180.ece>
2. Estimated by Zebi research team
3. <http://www.livemint.com/Politics/7MJYb4WJXezaRdf8Sr1ubl/Privacy-is-a-fundamental-right-says-Supreme-Court-in-histor.html>
4. <http://www.datacenterknowledge.com/data-center-world/bracing-change-brought-forth-gdpr>
5. <http://www.thehindu.com/news/national/centre-constitutes-new-panel-under-former-sc-judge-to-prepare-draft-data-protection-law/article19402660.ece>
6. <https://www.deccanchronicle.com/nation/current-affairs/161217/3-innovative-apps-to-up-amaravatis-expansion.html>
7. <http://www.india.com/news/india/reserve-bank-of-india-considering-to-introduce-its-own-cryptocurrency-similar-to-bitcoin-report-2478723/>

8. <https://technology.siliconindiamagazine.com/viewpoint/in-my-opinion/big-data-analytics-market-future-scope-in-india--nwid-9011.html>
9. Estimated by Zebi Research Team
10. <http://www.fonearena.com/blog/224741/jio-customer-database-of-over-120-million-users-leaked-could-be-biggest-data-breach-in-india.html>
11. <https://www.ndtv.com/business/aadhaar-data-breach-210-government-websites-displayed-private-data-says-uidai-1777380>
12. <http://www.orfonline.org/research/securing-property-rights-india-through-distributed-ledger-technology/>
13. <https://economictimes.indiatimes.com/small-biz/security-tech/security/zomato-hacked-security-breach-results-in-17-million-user-data-stolen/articleshow/58729251.cms>
14. <http://time.com/money/4936732/equifax-massive-data-breach-has-cost-the-company-4-billion-so-far/>
15. <http://www.livemint.com/Money/5FQtrxJC8jTi9EI5muZTRL/Identity-theft-biggest-contributor-to-fraud-Report.html>
16. <https://www.indiatimes.com/news/india/nearly-10-indians-lie-on-their-resumes-to-get-jobs-50-submit-fake-documents-330402.html>
17. <https://www.ndtv.com/business/airtels-aadhaar-sim-verification-faces-road-bump-as-uidai-suspends-e-kyc-licence-1788623>