CBS COPENHAGEN BUSINESS SCHOOL
HANDELSHØJSKOLEN

Elective Course on Mastering Blockchain: Foundations to Consensus, session-06

Blockchain Applications and Usecases

Raghava Mukkamala

Associate Professor & Director, Centre for Business Data Analytics
Copenhagen Business School, Denmark
Email: rrm.digi@cbs.dk, Centre: https://cbsbda.github.io/

Course Coordinator at SRMIST:

Prof. K. Shantha Kumari

Associate Professor
Data Science and Business Systems Department,
SRM Institute of Science and Technology, India
Shanthak@srmist.edu.in

EQUIS ACCREDITED AACSB ACCREDITED ASSOCIATION AMBA ACCREDITED CEMS PIM

Outline

- Project Ideas and Project Template Document

- Blockchain Applications and Use Cases
  - Blockchain for Social Business & Socio-Economic Development
  - Blockchain for Personal Data Management

Project Report Template

Image by MichaelWuensch from Pixabay

CBS

Project Guidelines

- Choose a decentralisation use case for which you want to apply blockchain technology.
- Use the knowledge gained in this course to come up with a conceptual design based on blockchain for your use case or develop a prototype implementation.
- Remember that your proposal could be a public blockchain or a protected blockchain, but substantiate it sufficiently with suitable arguments why you want go for it.
- May be code the Blockchain / smart contracts using one of the open source frameworks.

Report Guidelines - I

- **Introduction**
  - Motivation, Relevance and Research Question
- **Case study description**
  - What are the requirements of your use case?
  - What are the challenges you are trying to solve with blockchain?
  - What is the scope of decentralisation?
- **Methodology and Concepts**
  - Describe which methods/concepts you would like to use as part of your conceptual design

Report Guidelines - I

- **Conceptual Design**
  - Stakeholders
    - Who are the stakeholders of the system, and what are their roles?
    - What are their requirements?
    - How do they interact with the system, before and after?
  - Describe
    - Your proposed design elaborately explains the key features of your design
    - Try to argue why a feature is important and what advantage you get by using blockchain.
    - What are the system's use case scenarios?

Report Guidelines - III

- **Discussion**
  - How your proposed design satisfies your requirements?
  - How your design addresses the goals of decentralisation?
  - What are the opportunities your decentralised design will provide when compared to a centralised system?
  - What are the challenges you might have to solve if you want to implement your decentralised system
  - Most importantly answer your research question.

- **Conclusion and Future Work**
  - Conclude the project and mention how your design could be improved in the future, if some one wants to take it further

Use case-I: Blockchain for Social Business & Socio-Economic Development

Image by MichaelWuensch from Pixabay

CBS

Social Business

Social Business (SB): (NGO/NPO)

- business model for investments in social causes, such as poverty removal and welfare activities that are not attractive to traditional profit-based business models
- primary goal is the socio-economic development of the underprivileged
- SB gets funds from sponsors/social investors who may be individuals, philanthropic foundations, etc., to carry out the socio-economic development projects
- to continue sustained development activities, SB needs to have a continuous flow of funds from sponsors/social investors, which needs much trust in SB

Social Business

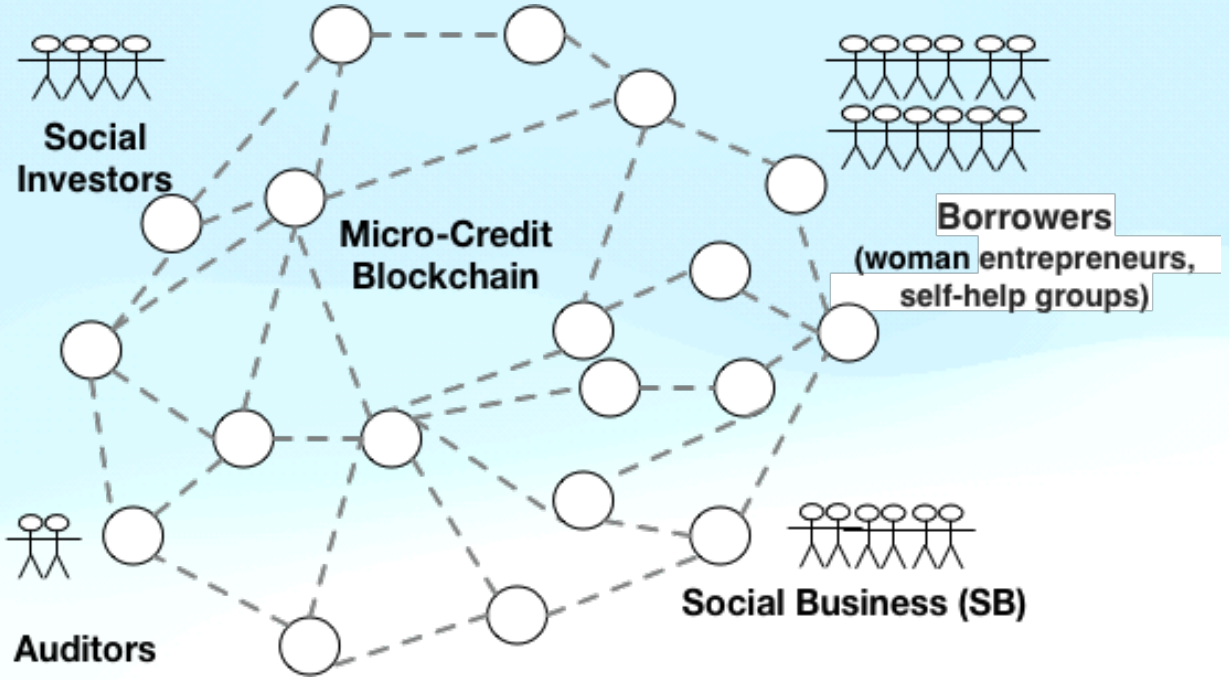
Social Business (SB): (NGO/NPO)

- Social Business (SB) is the term defined by Nobel laureate **Prof. Yunus** to develop a business model for investments for social causes such as poverty removal, healthcare, and welfare activities that are not attractive from the perspective of traditional profit-based business models.
- In this paper, we consider a Social Business that delivers micro-financing services from social investor funds to beneficiaries to generate livelihoods and promote social development.
- Traditionally, a micro-finance operating SB collects sponsorships from social investors and soft loans them to eligible borrowers for a pre-specified period of time for a pre-approved purpose.
- At the end of the period, the SB collects the maturity amount from the borrower and transfers it back to the social investor.

Research Question

How can blockchain technology help in addressing the challenges faced by Social Business organizations?

Use Case - Stakeholder Analysis



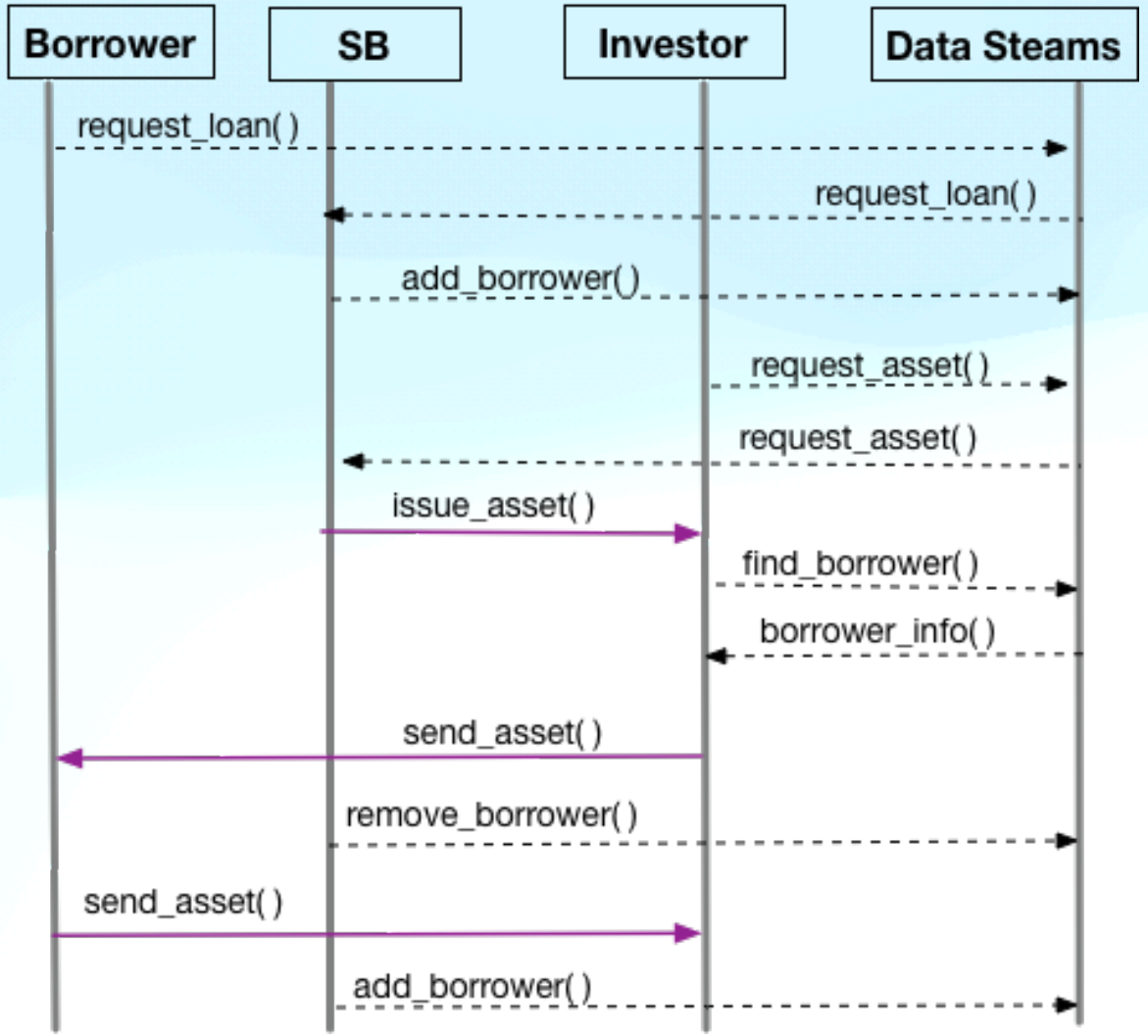
- Investors: Social investors who invest their money at 0% interest rate
- SB organisation selects women borrowers who need money for their small businesses
- Borrowers: Women from SHG, looking for loans of INR 10000-20000 ($150-300)
- Auditors: external people/entities/investors auditing the operations of fund

Conceptual Design

- Micro-credit blockchain as a permissioned blockchain (with public visibility) using MultiChain open source platform
  - to have control over who can perform a transaction (e.g. who can borrow) and which type of transactions.
  - to have a simple and inexpensive mining scheme (e.g. proof-of-publication) instead of having an expensive mining scheme like Bitcoin's proof of work
- cost of mining is negligible in permissioned blockchain very little computing resources (e.g. proof-of-publication)

Users	Permissions	details
Investor, borrower	send, receive	to send and receive assets.
SB	admin, issue, send, receive, mine	grant permissions to users, issue assets, mine blocks etc.
auditors, public	connect, mine	connect to see blockchain's contents, mine (verify transactions, create new blocks)

Borrowing Use-case in Blockchain



Borrowing Use-case in Blockchain

- Let us assume that n, b, i represents SB (e.g., NGO), borrower, and an investor, respectively in the blockchain
- $(p_n \mid s_n)$, $(p_b \mid s_b)$, $(p_i \mid s_i)$ (public | private) keys respectively of NGO, borrower and investor respectively
- Borrower requesting loan:
  - send_with_data(p_n, –, obj) where obj = {"for" : loan_requests, "amount" : 5000, "key" : p_b . . .}
- Investor obtaining an asset
  - issue(p_i, $asset_i$, 10000)
- Finding a borrower and transferring asset
  - send_asset(p_b, $asset_i$, 5000)

Opportunities with Blockchain

- **Trust Factors**: lot of trust into the operations of SB
  - assets/funds transfer to borrower (public key p_b) guarantees that only the borrower (the holder of respective private key s_b) can consume the asset, there by guarantees that no one else can receive the asset
  - use of underlying asymmetric cryptography will bring in authentication, integrity and non-repudiation of transactions and data
- **Transparency**: lot of transparency in operations of SB
  - public visibility of the blockchain (even though permissioned) allows any one can connect to the network/ download the contents to verify them
- **Privacy**: having transparency in the system does not necessarily leads to privacy violations
  - stakeholders interact with pseudonyms (keys), so until unless explicitly needed, their identities are completely hidden
  - Identities of SB, borrowers can revealed, investors identities concealed

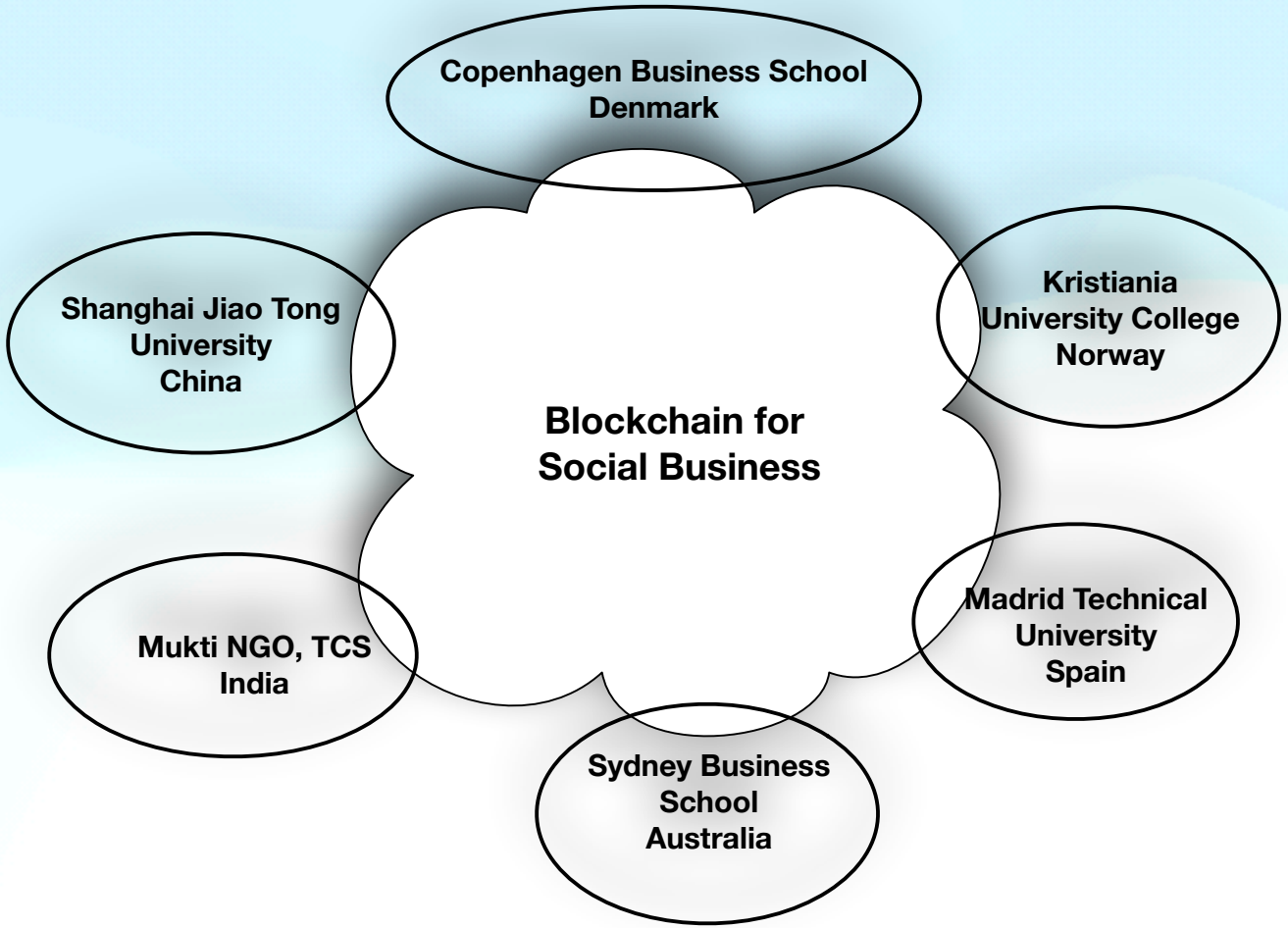
Opportunities with Blockchain

- **Decentralisation**: inherently distributed so few advantages
  - control over the or network is distributed across many entities (e.g. mining nodes), so no one (e.g. SB) can monopolise or compromise the network
  - Brings in robustness as the network avoids single point failure and easily be restored from the copy from a one-hop peer
- **Auditability** : many opportunities for auditing operations of blockchain
  - blockchain is like a digital bookkeeping system, recording all transactions, messages/data transfer in an immutable timestamped database,
  - E.g. one could verify whether there is any discrimination or partiality by SB in screening the borrowers, granting loans over a period of time as the auditors can get access to full immutable blockchain entries since start
  - auditors can also participate in the mining activities voluntarily + continuous monitoring possible

Challenges

- **Digital Asset / Cryptocurrency:** a native cryptocurrency
  - will have challenges related to exchange with Fiat & other cryptocurrencies and also need to deal/comply with lot of financial registrations/regulations
  - if anchored to an existing cryptocurrency (e.g. bitcoin) then need deal with all the uncertainties, volatilities and price fluctuations
- **Infrastructure and Deployment** :
  - SB needs to find suitable professional, technical help to develop the solution + needs suitable infrastructures and nodes to run and mine the blockchain at least initially
  - Some of the stakeholders (e.g. borrowers) might not have the access/ability to use computers, but only to the devices like mobile phones, so that needs developed light-weight mobile clients for blockchain that can run on basic mobile devices
- **Training and Adoption** : Adopting to new technologies like blockchain and smart contracts takes time and resources + need proper training and orientation to adopt to the new ways of interactions

Project Partners



Publications

Blockchain for Social Business: Principles and Applications

Index Terms—*Blockchain Technology, Social Business, Distributed Ledger Technology.*

Raghava Rao Mukkamala[1,2], Ravi Vatrapu[1,2], Pradeep Kumar Ray[3], Gora Sengupta[4] and Sankar Halder[4]
[1]Centre for Business Data Analytics, Dept. of Digitalization, Copenhagen Business School, Denmark
[2]Department of Technology, Kristiania University College, Norway
[3]University of Michigan-Shanghai Jiao Tong University Joint Institute, China, [4]Mukti, India
{rrm.digi,vatrapu}@cbs.dk, pradeep.ray@sjtu.edu.cn, {gora.sengupta,sankar.halder}@muktiweb.org

IEEE Engineering Management Review Journal (2018)

https://raghavamukkamala.github.io/files/pubs/2018_Blockchain-Social-business-Principles-Applications.pdf

IEEE Big Data Conference (2018)

Converging Blockchain and Social Business for Socio-Economic Development

Raghava Rao Mukkamala[1,2], Ravi Vatrapu[1,2], Pradeep Kumar Ray[3], Gora Sengupta[4] and Sankar Halder[4]
[1]Centre for Business Data Analytics, Dept. of Digitalization, Copenhagen Business School, Denmark
[2]Department of Technology, Kristiania University College, Norway
[3]Shanghai Jiao Tong University (SJTU), China [4]Mukti, India
{rrm.digi,vatrapu}@cbs.dk, pradeep.ray@sjtu.edu.cn, {gora.sengupta,sankar.halder}@muktiweb.org

https://raghavamukkamala.github.io/files/pubs/2018_IEEE_BigData_Blockchain_social_business.pdf

Use case-II: Blockchain for Personal Data Management

BPDIMS:A Blockchain-based Personal Data and Identity Management System

Benedict Faber, Georg Michelet, Niklas Weidmann, Raghava Rao Mukkamala, Ravi Vatrapu
Associate Professor, Centre for Business Data Analytics (bda.cbs.dk)
Department of Digitalization, Copenhagen Business School, Denmark
Email: rrm.digi@cbs.dk

Associate Professor, Department of Technology,
Kristiania University College,Oslo, Norway

Hawaii International Conference on System Sciences (HICSS)
MAUI, Hawaii, USA
2019-01-11

CBS

Overview

- Motivation
- Theoretical Foundations: Blockchain, GDPR, MyData
- BPDIMS Conceptual design
- Use Cases and Discussion
- Conclusion

Motivation

- Our lives have become increasingly digital, as have the vast number of personal data traces we leave behind on digital platforms..
- Few large multinational corporations (like Facebook, Twitter, and Instagram) make the majority of profits by offering services that users pay for with their data.
- Users' overview and control over their personal data have decreased.
- The Cambridge Analytica scandal to influence voters in US Elections has raised concerns about the technical, commercial, political, and ethical aspects of personal data

Personal Data Management

- Recent EU GDPR law aims to give control of personal online data to European users through new regulation.
- Several initiatives (such as MyData[1]) have been launched both from private and public spheres, to argue for a human-centric approach to personal information
- MyData facilitates the human-centric approach to people's data which argues that the users should have a better overview of where their data is stored, who uses it, and be able to change this.
- Blockchain attracted research and industry attention due to its disruptive characteristics, such as the absence of centralised control and high degree of anonymity

1) A. Poikola, K. Kuikkaniemi, and H. Honko, "Mydata a nordic model for human-centered personal data manage- ment and processing," Finnish Ministry of Transport and Communications, 2015.

Research Question

- Currently, users lack transparency over which service is processing their personal data for which purpose.
- Lack of systems that enable users to obtain an overview of the usage of their personal data and to exercise fine-grained control over the usage of their personal data.

How can blockchain be used to develop a human-centric, GDPR-compliant system for personal data and identity management?

Related Work

- Automated access-control manager using Blockchain for a decentralised personal data management system [Zyskind & Nathan, et al. 2015]

- A privacy-preserving architecture with auditable contracts on blockchain for a transparent data access and sharing [Kaaniche and Laurent 2017]

- An architecture based on blockchain and on artificial intelligence for control of their personal health data including medical records [Mamoshina et.al. 2018]

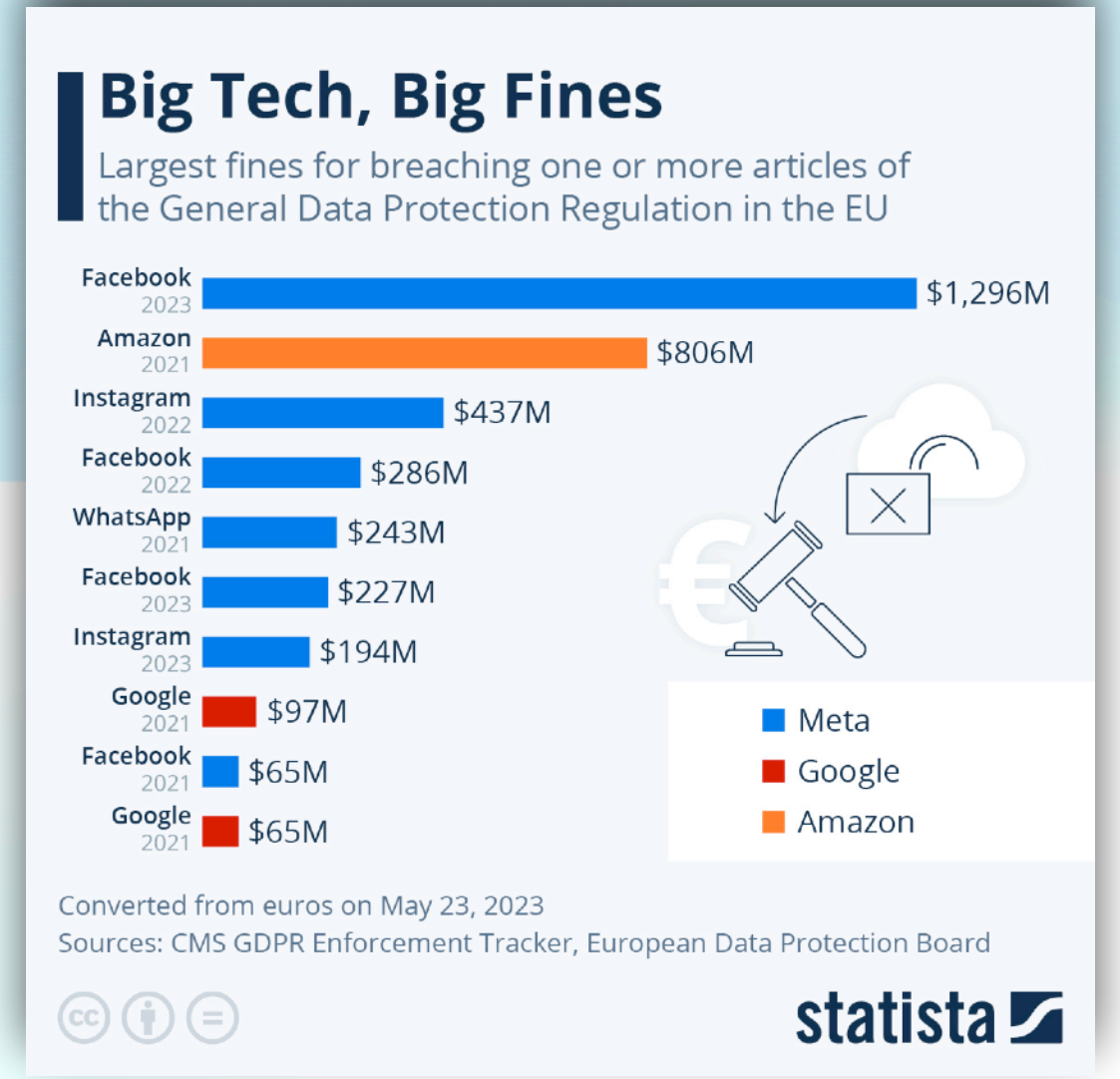
Foundations - Blockchain

- Applications that could previously run only through a trusted intermediary, now using blockchain can operate
  - in a decentralised fashion, by eliminating / limiting the need of a central authority,
  - achieve the same functionality with the same amount of certainty
- Blockchain enables trustless networks, since parties can transact even though they do not trust each other
- Heavy use of cryptography in blockchain, brings authoritativeness behind all the interactions by providing guarantees for immutable, tamper-resistance of transactions/records
- Smart contracts self-executing scripts over blockchain allow for proper, distributed, heavily automated workflows

Foundations - GDPR

- GDPR is the largest change in data privacy regulation in EU and came into effect in May 2018
- Aims to harmonise data privacy laws across Europe and particularly to empower and protect EU citizens' privacy
- Service provider must show what the user's consent is for and it should be easy for a user to withdraw his consent
- If user withdraws his consent, then the service provider required to delete the data related to the specific user
- The service providers must provide all data to the user in a machine-readable format
- Violations of GDPR can result in fines for companies of up to 20 million Euros or 4% of global turnover, whichever is larger

GDPR Fines in Europe



- Facebook paid ~ 16 000 Crores INR
- Amazon ~ 7 000 Crores INR
- Instagram ~ 5 000 Crores INR
- Google ~ 1 700 Crores INR

Foundations - MyData

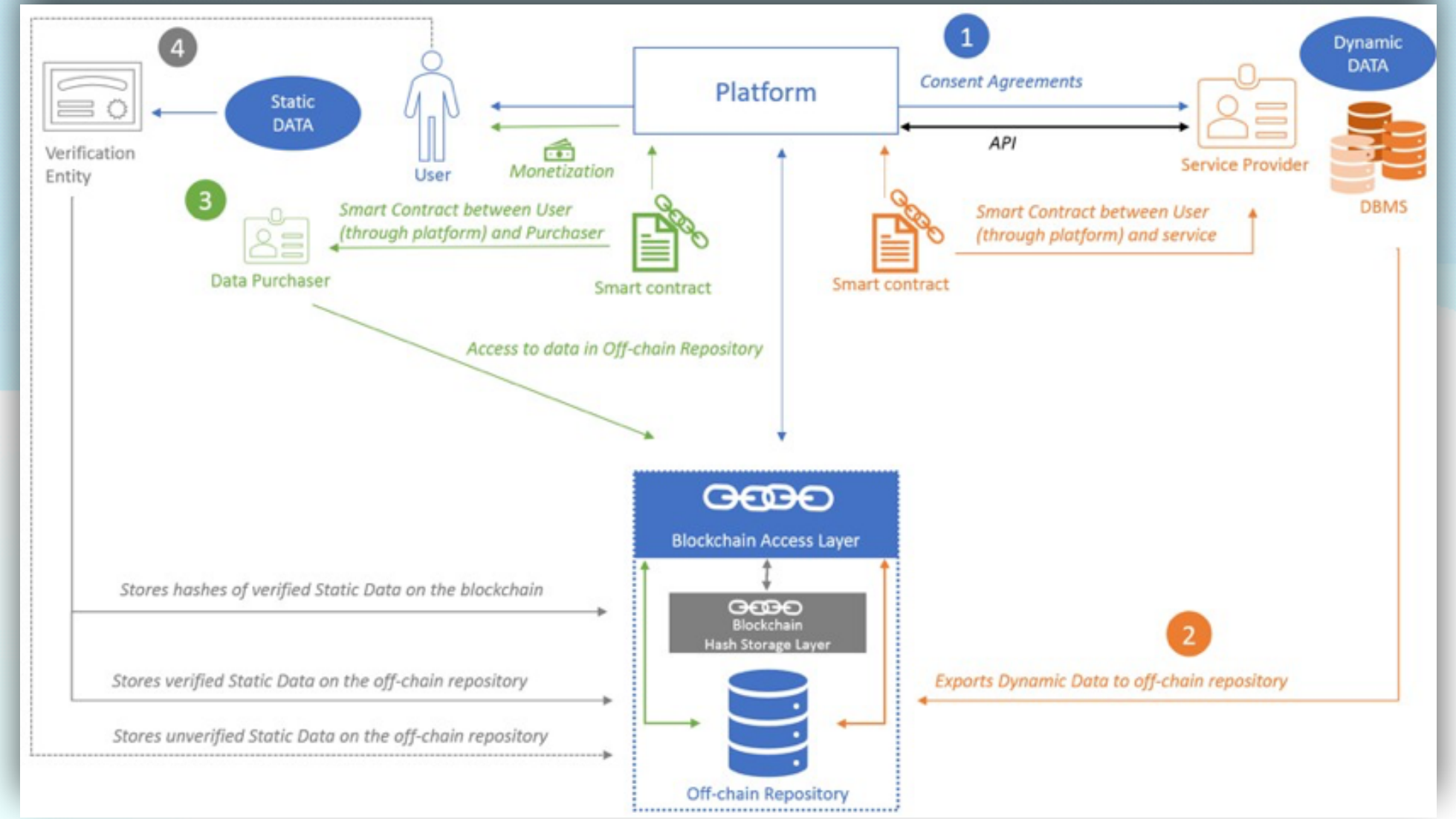
- Human-Centric Personal Data Management
- Main objectives from the user perspective are:
  - ✓ right to know what personal information exists,
  - ✓ right to see the content of personal information,
  - ✓ right to rectify false personal information,
  - ✓ right to audit who accesses personal information and why,
  - ✓ right to obtain personal information and use it freely,
  - ✓ right to share/sell personal information to others
  - ✓ right to remove or delete personal information

A. Poikola, K. Kuikkaniemi, and H. Honko, "Mydata a nordic model for human-centered personal data manage- ment and processing," Finnish Ministry of Transport and Communications, 2015.

Characteristics of Blockchain

Immutability	Data written to database cannot be changed or deleted without consensus leading to data integrity
Decentralization	No single point of failure/control achieved by decentralized architecture and a distributed database
Transparency	All data sent through the blockchain is visible to all network participants
Pseudonymity	The identity of data senders and receivers is unknown
Chronology	Every transaction is time-stamped and can be traced back

System Architecture



Design Guidelines

- User-centric: empowering the user
- Transparency: The user knows how and who has his data
- New rights: GDPR-compliant give and revoke consent
- Data economy: facilitates the trading of his own data by the user
- Validated data: validation of user data by data validators
- Security: user data in encrypted form with secure storage of encryption keys

Stakeholders & Roles

- **User**: end users utilizing the system
- **Service provider**: a company providing a service to a user (e.g., Facebook)
- **Data purchaser**: an entity purchasing the user data
- **Data validators** are entities that validate user data to ensure that it contains what the user claims to be.

System Components

Blockchain Layers

- Smart contract layer (Smart Contract Blockchain)
- Access layer (Access Blockchain)
- Hash storage layer (Identity Blockchain)

Off-chain repository:

- user data stored in encrypted form in cloud storage with hash pointers

User Interface (UI):

- to give an overview of all user's personal data
- to be able to manage all the data and consents

Use Case - Consent Management

Give consent to service provider:

- User agrees to terms and conditions of service provider (gives consent)
- System sends request to service provider for all the user's personal data.
- Service Provider sends data to the system in a commonly-used and machine-readable format.
- System is updated with info from the service provider and displayed in the user's UI.
- If purpose for data processing changes, service provider must ask for new consent

Revoke consent from service provider:

- User removes consent through UI.
- System sends request to service provider to stop processing and delete personal data regarding the user.
- System receives confirmation of deletion from service provider.
- System deletes the information from interface and/or repository, based on user's demands.

Use Case - Data Monetisation

Listing a dataset for sale:

- User gives consent to some data, if any, can be sold in the user interface.
- System lists this data as for sale in the marketplace.
- Data will be validated by the data validator who validate the claims of user data
- Certification of the data provides confidence to the data purchasers
- Consent is put into smart contract between user and data purchaser, pointing to the data in question.

Data purchaser buys data:

- Data purchaser can browse through the marketplace and select datasets he wants to purchase.
- Consent transaction is created on the access blockchain and together with the data pointer, compensation and expiry date stored in a smart contract
- The compensation is transferred to the user
- The data purchaser gets access to the repository and can download data

Discussion

Improvements Using Blockchain:

- Blockchain stores the hashed data pointers pointing to the user data on off-chain repositories, which provides guarantees that data has not been altered
- Blockchain provides transparency and verifiable proofs for transactions of user data and identity, which will enhance trust and confidence to all stakeholders: users, service providers and data purchasers etc.

Smart Contracts:

- Introduction of smart contracts for creating/revoking consents will result in unambiguous legal contracts
- Easy for auditors to investigate the claims in case of disputes between the users and service providers/data purchasers

Discussion

Encrypted Data Storage:

- the system avoids a single point of failure as user data is in encrypted form and the encryption key is distributed over different key keepers using threshold encryption methods
- A compromise of the off-chain data repository will not lead to a data leakage.

User's Perspective:

- users able to grant and revoke access to personal data, also monitor who has access to it, what it is being used for

Business Perspective:

- Compliance with the GDPR in dealing with both consent and data handling for service providers
- Possibility of buying data provides a significant opportunity for companies to expand and improve services

Conclusion & Future work

- We proposed a conceptual design and high-level architecture for a personal data and identity management for control over the usage of the personal data of users
- Building on the foundations of blockchain and smart contract with a human-centric focus, the proposed system provides high-level trust and security
- We would like to use a formal methods approach to derive a detailed and unambiguous specification and develop a prototype using one of the open source blockchain frameworks

Thank you!

Raghava Mukkamala

rrm.digi@cbs.dk

https://www.cbs.dk/staff/rrmdigi

https://raghavamukkamala.github.io/

https://cbsbda.github.io/