



ifj

University of Oslo (UiO)
Networks and Distributed Systems (ND)

Credence workshop in Stavanger, August 2019

1




UNIVERSITY
OF OSLO

Outline

- UiO presentation (aka boring stuff)
 - Projects
 - People
 - Application areas
 - Industry collaborations
 - Courses and teaching
- Current and past research focus
- Ideas for the stuff we could do together!



ifj

2



UNIVERSITY
OF OSLO

Projects (apart from Credence)

- **SmartMed:** Secure and accountable sharing of medical records using smart contracts and blockchain 
 - national project granted for 4 years
 - In collaboration with the Cancer registry of Norway (records for over 1,4 mil cancer patients)
 - 2 postdocs, 2 PhD students, and one engineer
- **Conserns:** strategic research initiative for information security research 
 - 5 research groups at UiO
 - Funded ~10 PhD students and postdocs over six years



3



Research Projects (continued)

- **SmartNEM:** Smart Community Neighborhood - driven by energy informatics
 - Goal: to develop new models and algorithms to provide the power grid operators with intelligent energy management with privacy preservation in local regions
 - Duration: 2017-2021
 - Funding: 25 MNOK (20M by RCN)
- **DILUTE:** Fluid Service Abstraction for Large-Scale Cloud IoT Systems
 - Goal: to devise a unified IoT services development and management framework for large-scale and dynamic IoT applications, built over fogs and the Cloud
 - Duration: 2018-2021
 - Funding: One PhD and one postdoc



Workshop attendees from Oslo



Andrea Merlina
PhD student
Blockchain, ML



Mohammad Tabatabaei
PhD student
Blockchain



Amir Taherkordi
Postdoc
IoT, Sensors



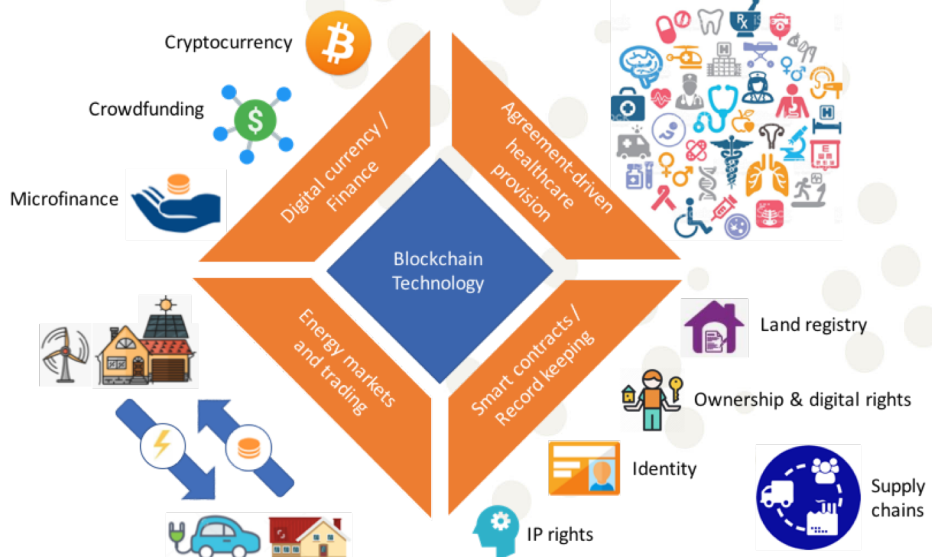
Dapeng Lan
PhD student
Fog services
Smart cities



Vinay Setty
Former PhD
Now faculty
at UiS
ML, Social
notifications



Application areas related to blockchain



Area: Smart Cities

- **Transport** planning and optimization
- **Energy** management and trading
 - Charging **electric vehicles**
- **Data sharing** across municipality services and departments
- Managing **contracts** and tracking their execution
- **Welfare** and **healthcare** management
- Cutting on **bureaucracy**



7

UNIVERSITY
OF OSLO

Sample Research Questions for Smart Cities

- How to enable **interoperable data sharing** and **analytics across fragmented services** and infrastructures and **across data silos**?
- How to resolve issues of **data ownership** and **usage**, **data quality**, **data protection** and **privacy**, **security**, and **liability** considering both **industry data**, **public data**, **sensor data** and **personal data**?
- What are appropriate **business models** when considering **data as an economic asset** ?
- Social research questions: How to **engage the citizen** in smart city development?



8

UNIVERSITY
OF OSLO

Industry collaborations

- Blockchain
 - **IOTA** (smart cities, tangle algorithms)
 - **IBM Hyperledger** team
 - National: blockchangers, Norwegian BX, etc.
 - Norwegian State Educational Loan Fund
- Other in Norway and Europe
 - **SAP** (business models, smart cities)
 - **DNB** and other banks
 - **Spotify** (social notifications)
 - Other related to energy and smart cities



Courses and tutorials

- An introductory course to distributed systems
 - Master level
 - Given every fall
 - Frontal lectures and 3 programming assignments
 - Always looking for new assignments
- An advanced seminar in blockchain
 - For graduate students
 - Reading, presenting, and discussing papers
 - Looking for new papers and programming elements
 - Especially about system design
- A five hour long tutorial on blockchain
 - Developed together with Kaiwen, Mohammad, and others
 - Presented at DEBS, Middleware, summer schools
 - Includes a hands-on section in addition to covering the concepts

Recent research topics: blockchain

- Data storage and sharing in healthcare (2PhD+2PD+1E)
- Replacing PoW with machine learning tasks (one PhD)
- Understanding blockchain properties (one PhD)
 - In-depth comparison of popular systems
 - Taxonomies, analysis, experimentation
 - Education of masses: debunking blockchain myths
- Benchmarking blockchain systems (2 MSc students)
 - Good utilities for some specific systems
 - No cross-system tools
- Devising new algorithms for IOTA Tangle



11



Topic: data sharing in health and welfare

Support for shared data storage is vital

- High number of life-threatening medical errors because of inaccessible information
- Required for a holistic health and welfare
 - A lot of data sources
 - Integration with data monitoring devices
- Needed for patients travelling abroad
- Provision for analytics
 - Sharing is the only way to develop new medicines

yet challenging ...

- A frequent target for security attacks
- Who owns the data?
- Bridging over isolated silos
- Subject to a large number of national and European regulations
 - What data can be stored where
 - Managing consent by the data owner
 - Obligation to report to the data owner/patient about accesses
- Requires advanced access control schemes
- Privacy of the data
 - Qualified privacy
 - Generation of synthetic datasets



Topic: replacing PoW cryptopuzzles with ML tasks (Andrea's PhD)

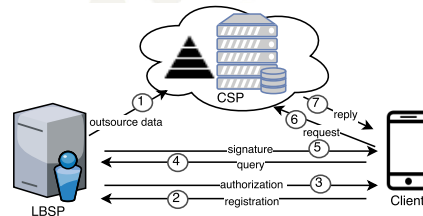
- PoW is hugely **wasteful**
- **Idea:** replace cryptopuzzles with ML tasks
- **Challenging:** has to satisfy many properties
 - Useful ML tasks cannot be totally random
 - Yet must depend on the set of transactions
 - The complexity must be controllable
 - The model has to deal with training and test data
 - The test data is usually disclosed later than the task
 - A solution to an ML task is never perfect
 - Has an accuracy threshold
 - Validation must be efficient

Older research topics

- Privacy-preserving outsourcing to the cloud
- Privacy-preserving group communication
- BFT, reconfiguration and similar
- Social notifications and pub/sub
- Performability

More fleshed out yet perhaps less relevant!

Privacy-preserving outsourcing to the cloud (one PhD thesis)



- **Application domains:** location data, genomic datasets
- **Query models:** similar patients, proximity-based
- **Threat model:** the cloud is honest but curious
 - Would love to run analytics on the data and queries
 - Necessitates the search over encrypted data
- **Solution elements:** new index structures, quantifiable privacy, semantic security, scalable key maintenance
- **TDSC 2018**, another paper in submission

Privacy-preserving group communication (one PhD thesis)

- Protecting identities, messages, and membership info
- Threat model: curious ISPs, group members, and onion routing proxies
- Limited support for multicast in Tor
- Problem 1: Scaling onion routing with the number of groups
- Problem 2: Combining F2F communication with onion routing
- Problem 3: Better selection of onion routing proxies
- ICDCS 2012, another paper in submission

Social notifications (one thesis +)

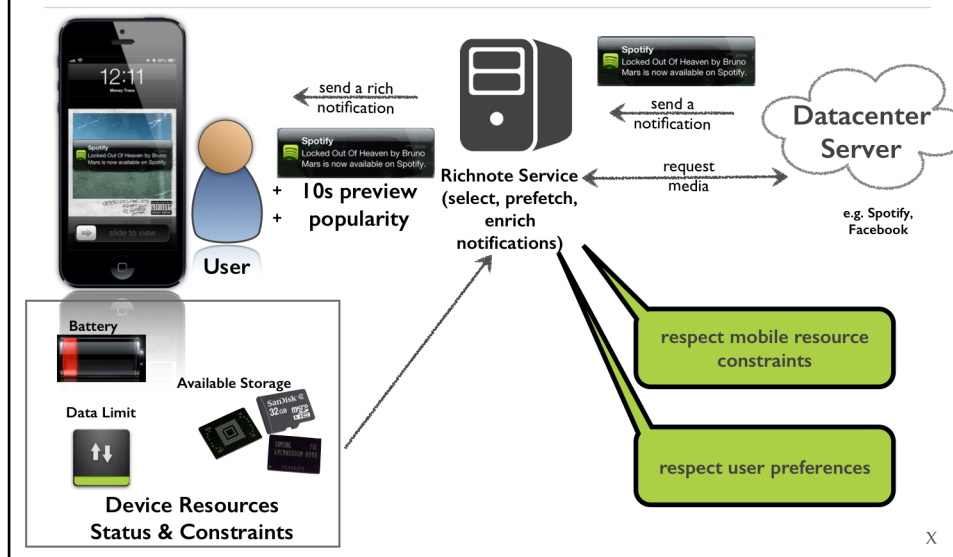
- Too many short notifications on mobile phones
 - Need to select and prioritize
- Barebone textual messages limit user's selection ability
- Pulling media content from URL in notifications incurs **latency** and counts against **mobile data plans**
- Solution elements:
 - **Utility model** for content and presentation
 - **Select content items and presentation** levels so as to maximize utility, while respecting resource constraints
 - **Scheduled delivery** of notifications



17



Proposed: Rich Media Notifications



Amir Taherkordi's research topics

- Dynamic and Scalable Service Distribution in Fog-Cloud Platforms



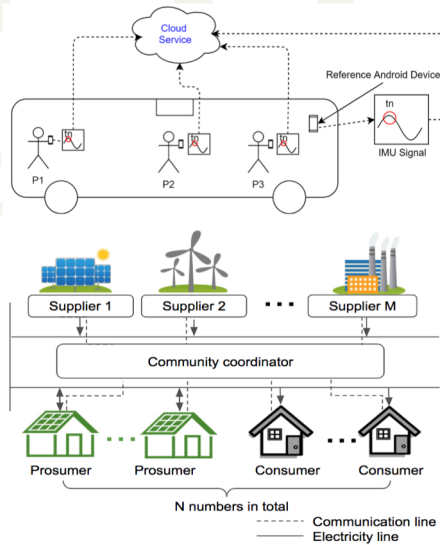
- Cross-Cloud Big Data Processing



Amir Taherkordi's research topics

- Intelligent Location-Driven Mobile Systems

- Mobile Recommender Systems
- Machine Learning for Mobile Context Detection



Directions for future collaboration (blockchain)

- Developing core blockchain technologies
 - Improving Hyperledger, IOTA, or Ethereum
 - Coming up with new algorithms and systems
 - Consensus, storage, communication layers
- Developing blockchain applications
- Contributing to the smart contract ecosystem
- Ledger-enhanced storage systems
- Taxonomies, analysis of blockchain systems



21



Directions for future collaboration (other)

- Dark Internet (Tor, Aqua)
- Privacy-preserving outsourcing to the cloud
- Consensus and replication beyond blockchain
- Building dependable applications beyond blockchain



22



Ideas for future collaboration (research)

- Standard must have stuff
 - **Student mobility!!!**
 - **Pairing of students** tasked with a project
 - Hopefully resulting in publications
 - **Joint supervision**
 - **Research visits** and stays for the faculty
 - **Popular science articles**
- Ambitious/high aim
 - Potential for **cross-disciplinary** research
 - Organizing a **workshop** collocated with a conference?
 - Perhaps a **Dagstuhl seminar**?
 - Write a **collection book**?

Ideas for future collaboration (education)

- In addition to the **promised summer school**
- **Visiting and remote lectures**
- Develop a **joint blockchain course**
- Development of programming assignments/projects (e.g., in blockchain)
- **Educational software** (e.g., for learning BC)
- **Specialized tutorials**

Questions?



25



UNIVERSITY
OF OSLO