Responsible Use of AI and Blockchain in Telecommunications

Jason Hunt

IBM Distinguished Engineer

@DJHunt

Open Networking Summit 2019

IBM

Today

Bias and Fairness in AI

Power and Privacy in Blockchain

Lessons for NFV

02.13.18

Facial Recognition Systems Are Even More Biased Than We Thought

AI from Microsoft, IBM, and Face ++ is much less accurate when detecting dark-skinned female faces than light-skinned male faces.

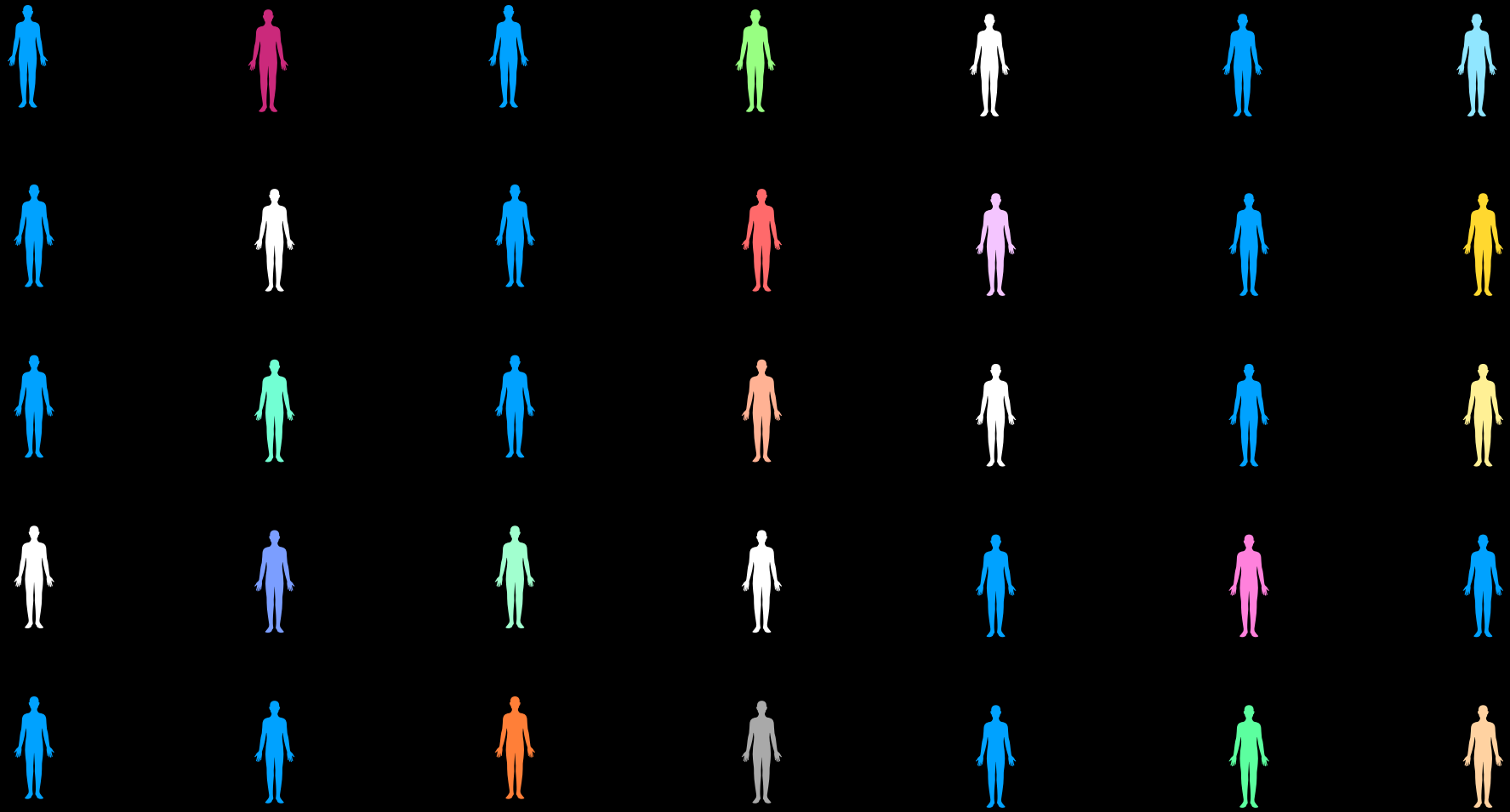
Intelligent Machines

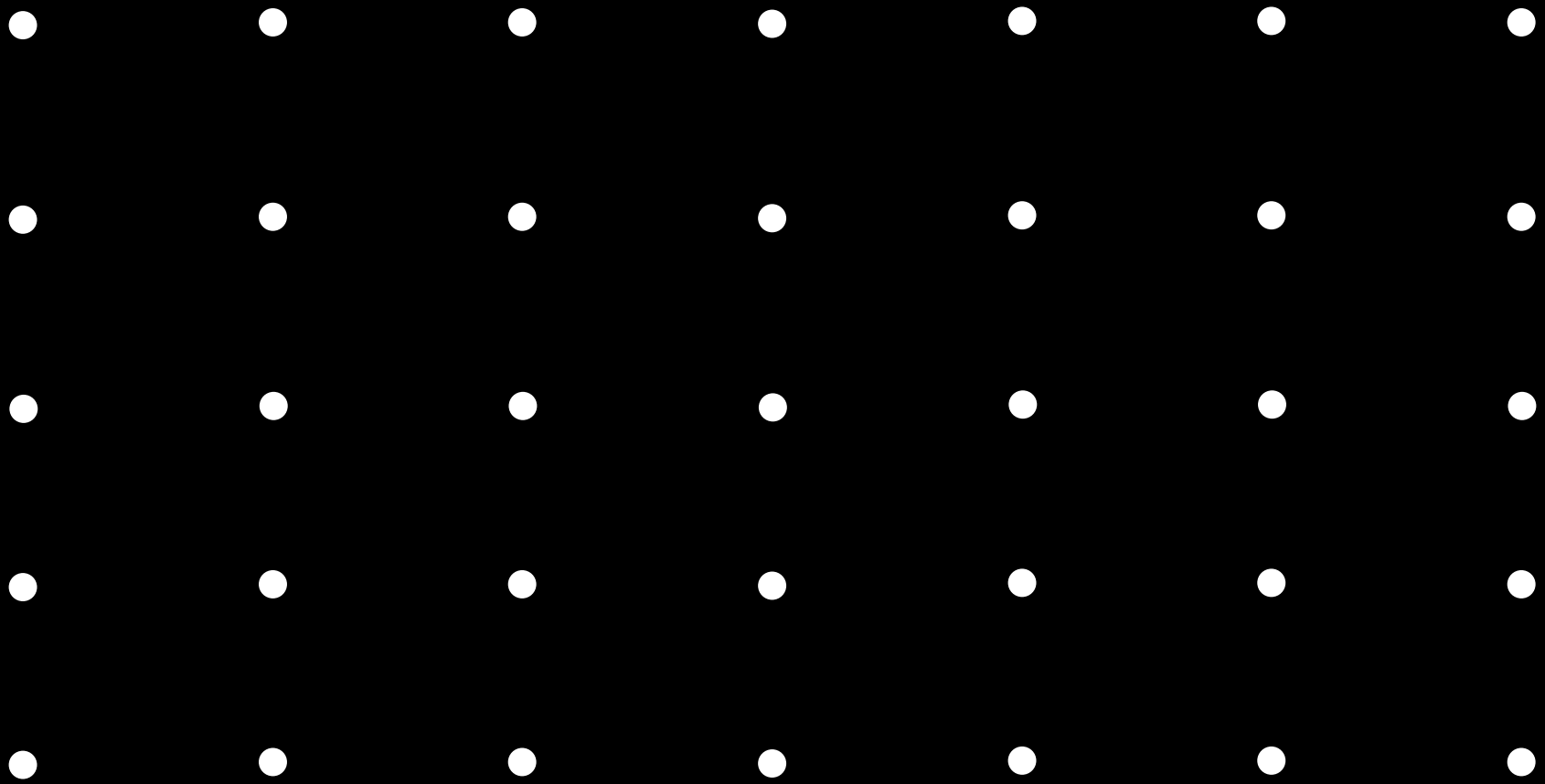
Forget Killer Robots—Bias Is the Real AI Danger

John Giannandrea, who leads AI at Google, is worried about intelligent systems learning human prejudices.

more data

less trust





As designers of programs, systems, and services, **we fail when we turn humans into statistics and data points.**

Ethical decision-making isn’t just another form of technical problem solving.

We are responsible for teaching machines what we value

ibm.biz/everydayethics

Five Focus Areas

1. Accountability
2. Value Alignment
3. Explainability
4. User Data Rights
5. Fairness

What is unwanted bias?

Group vs individual fairness

Machine learning is always a form of statistical discrimination

Discrimination becomes objectionable when it places certain **privileged** groups at systematic advantage and certain **unprivileged** groups at systematic disadvantage

Illegal in certain contexts

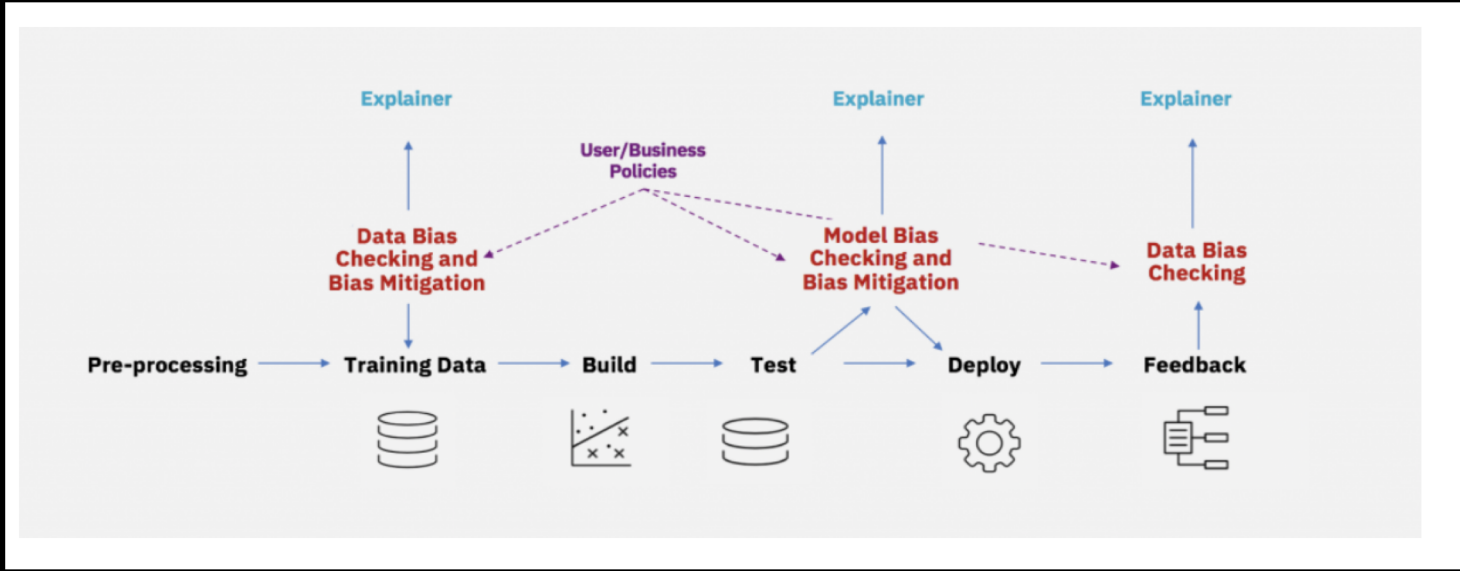
Where does it come from?

Unwanted bias in training data yields models with unwanted bias that scale out

Discrimination in labelling

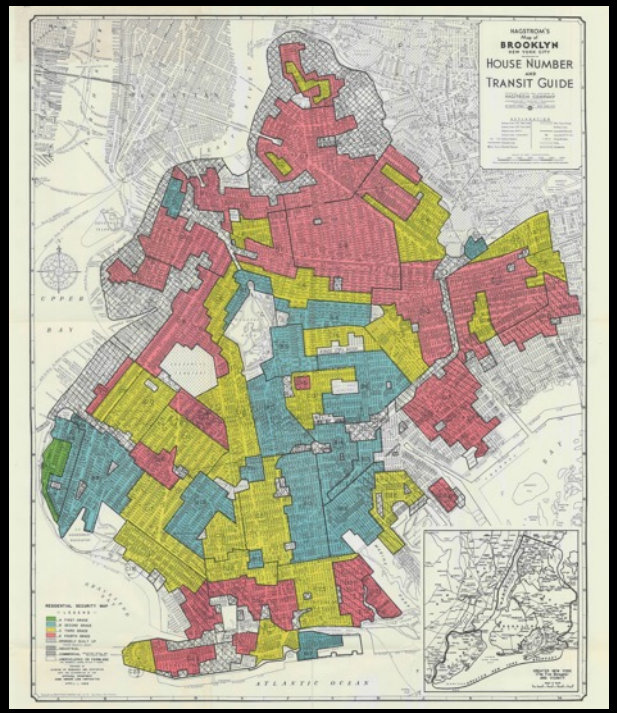
Undersampling or oversampling

Checking and Mitigating Bias throughout the AI Lifecycle using Metrics, Algorithms, & Explainers



Bias mitigation is not easy

Cannot simply drop protected attributes because features are correlated with them



AI Fairness 360

Datasets

Toolbox

- Fairness metrics (30+)
- Fairness metric explanations
- Bias mitigation algorithms (9+)

Guidance

Industry-specific tutorials

Differentiation

Comprehensive bias mitigation toolbox
(including unique algorithms from IBM Research)

Several metrics and algorithms that have **no available implementations** elsewhere

Extensible

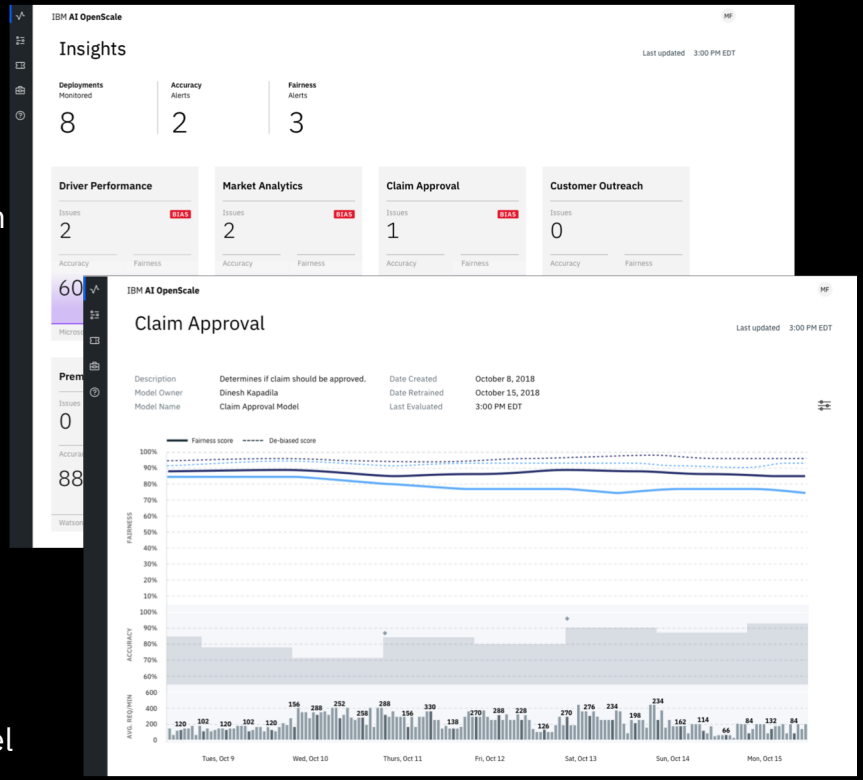
Designed to translate new research from the lab to industry practitioners

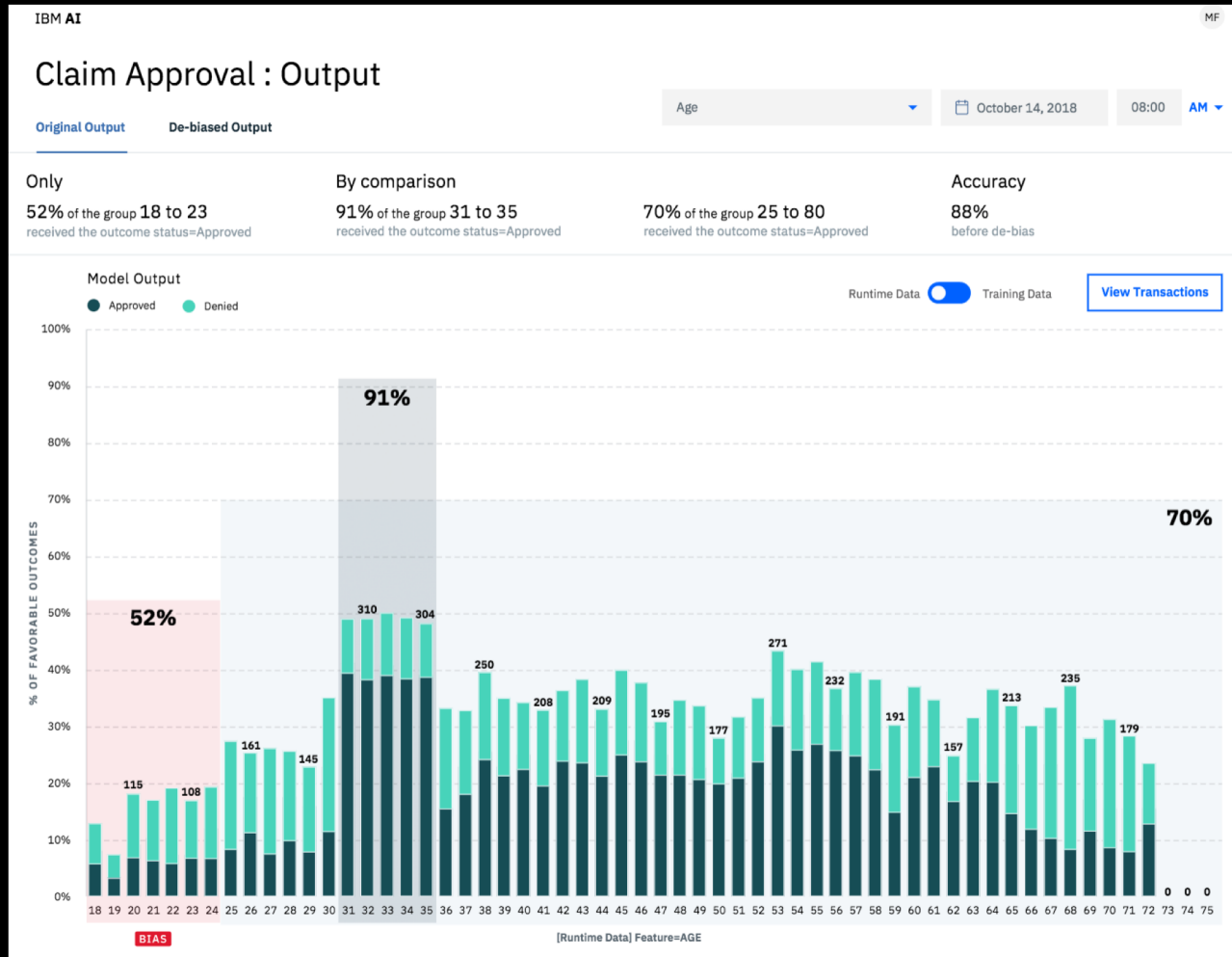
AI Fairness 360 Demo

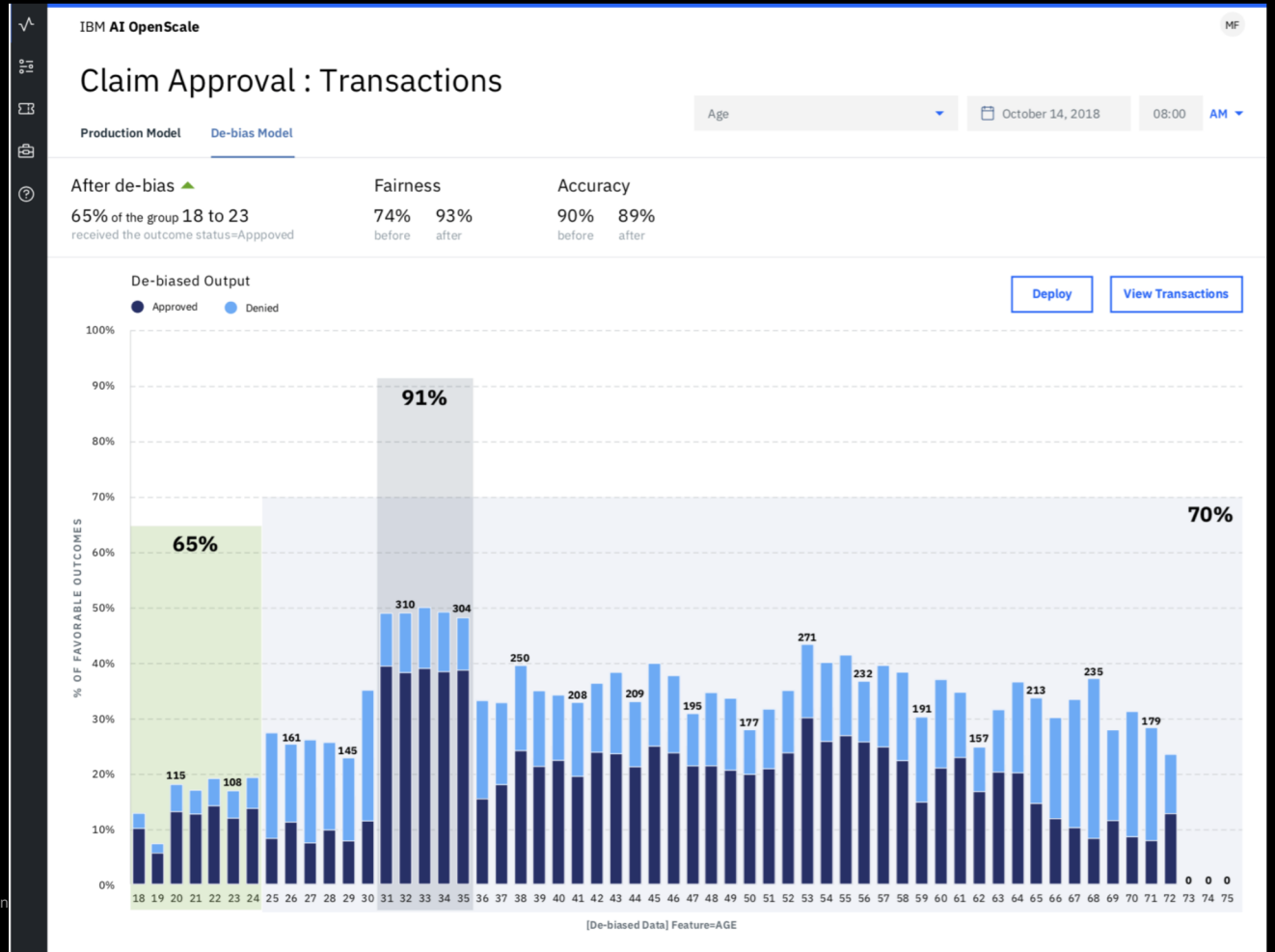
http://aif360.mybluemix.net
https://github.com/ibm/aif360
https://pypi.org/project/aif360

IBM Watson OpenScale
Automate and Operate AI at Scale

- Trust and Transparency
  - Intelligently delivers bias mitigation help
  - Provides traceability & auditability of AI predictions made in production applications
  - Tracks AI accuracy in applications
  - Explains an outcome in business terms
- Automation
  - Automatically detects and mitigates bias in model output, without affecting currently deployed model or outcomes
  - NeuNetS (beta) – automatically generate Neural Networks
- Open By Design
  - Monitor and optimize models deployed on third party model serve engines
  - Deploy behind enterprise firewall or on IaaS provider







Power and Privacy in Blockchain

Energy Usage of Blockchain

MARKETS

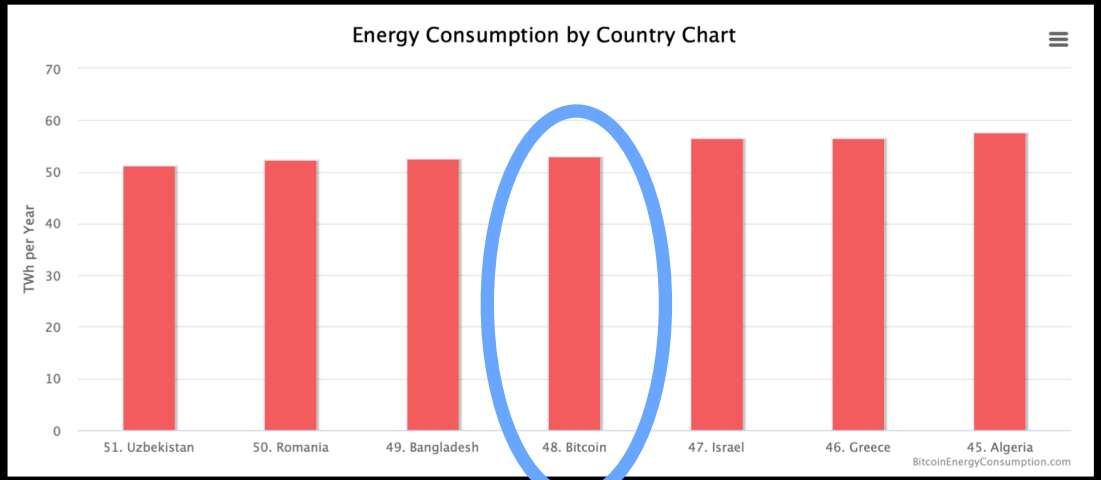
Bitcoin in the Wilderness

On a Canadian oil field, natural gas with nowhere to go powers a bitcoin-mining operation

By Stephanie Yang

Updated March 29, 2019 11:56 a.m. ET

https://www.wsj.com/articles/bitcoin-in-the-wilderness-11553860802



http://BitcoinEnergyConsumption.com

Consensus Approaches

TABLE 1. COMPARISON OF PERMISSIONED CONSENSUS APPROACHES AND STANDARD PoW

	Permissioned Lottery-based	Permissioned Voting-based	Standard Proof of Work (Bitcoin)
Speed	●●●●● GOOD	●●●●● GOOD	● POOR
Scalability	●●●●● GOOD	●●● MODERATE	●●●●● GOOD
Finality	●●● MODERATE	●●●●● GOOD	● POOR

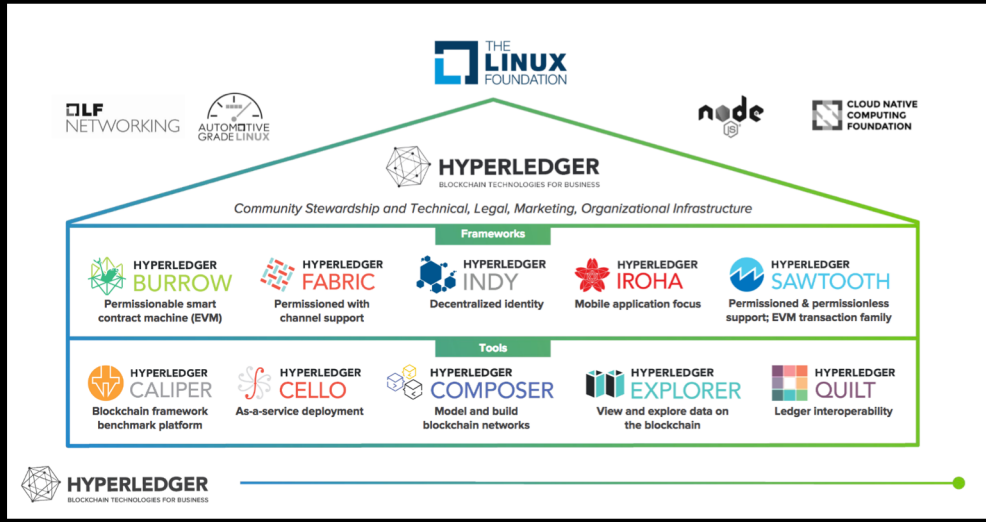
https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf

Hyperledger Project – Hyperledger Fabric

An implementation of blockchain technology that is intended as a foundation for developing blockchain applications

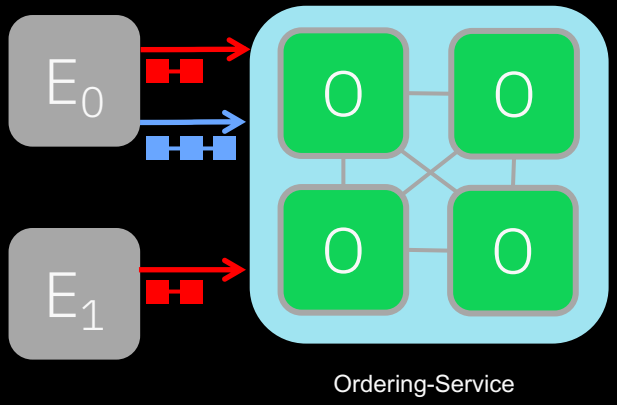
Key technical features:

- A shared ledger and smart contracts implemented as “chaincode”
- Privacy and permissioning through membership services
- Modular architecture and flexible hosting options



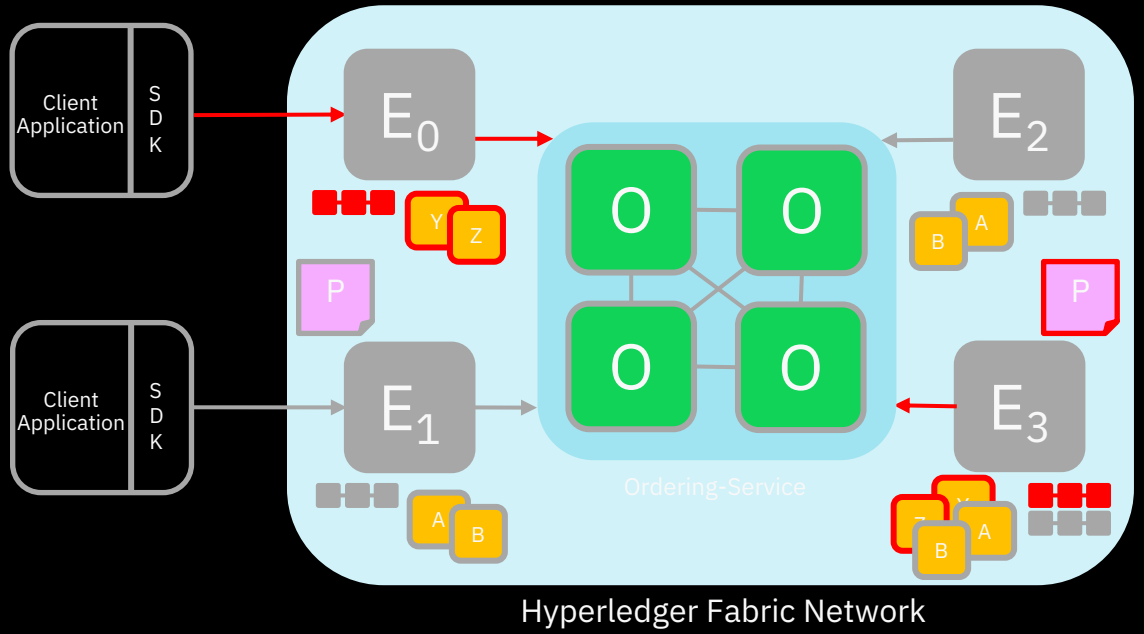
Channels

Channels provide privacy between different ledgers



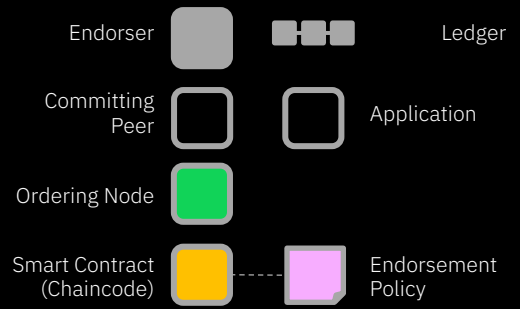
- Ledgers exist in the scope of a channel
  - Channels can be shared across an entire network of peers
  - Channels can be permissioned for a specific set of participants
- Chaincode is installed on peers to access the worldstate
- Chaincode is instantiated on specific channels
- Peers can participate in multiple channels
- Concurrent execution for performance and scalability

Multi Channel Network



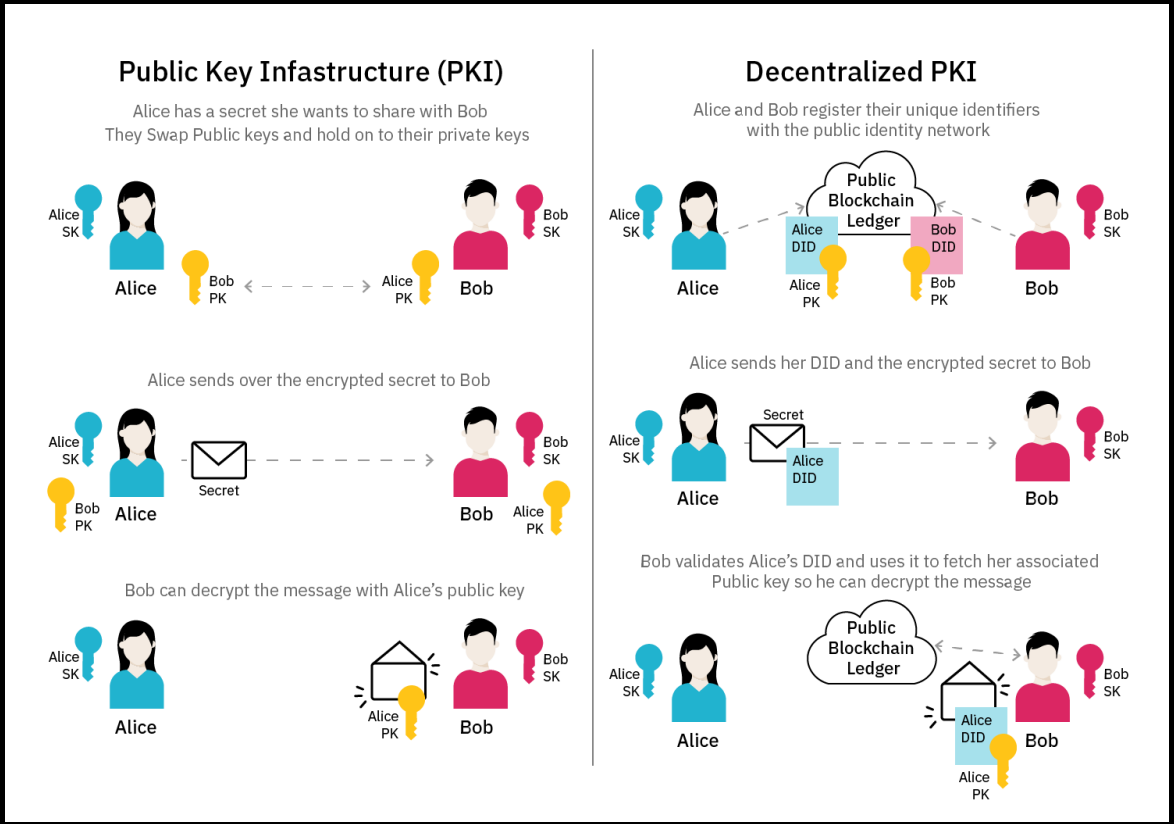
- Peers E_0 and E_3 connect to the red channel for chaincodes Y and Z
- E_1, E_2 and E_3 connect to the blue channel for chaincodes A and B

Key:



Self-Sovereign Identity: Why blockchain?

Blockchain technology is a catalyst for rebooting the web of trust vision by providing an infrastructure of identity attestations that is publicly accessible.



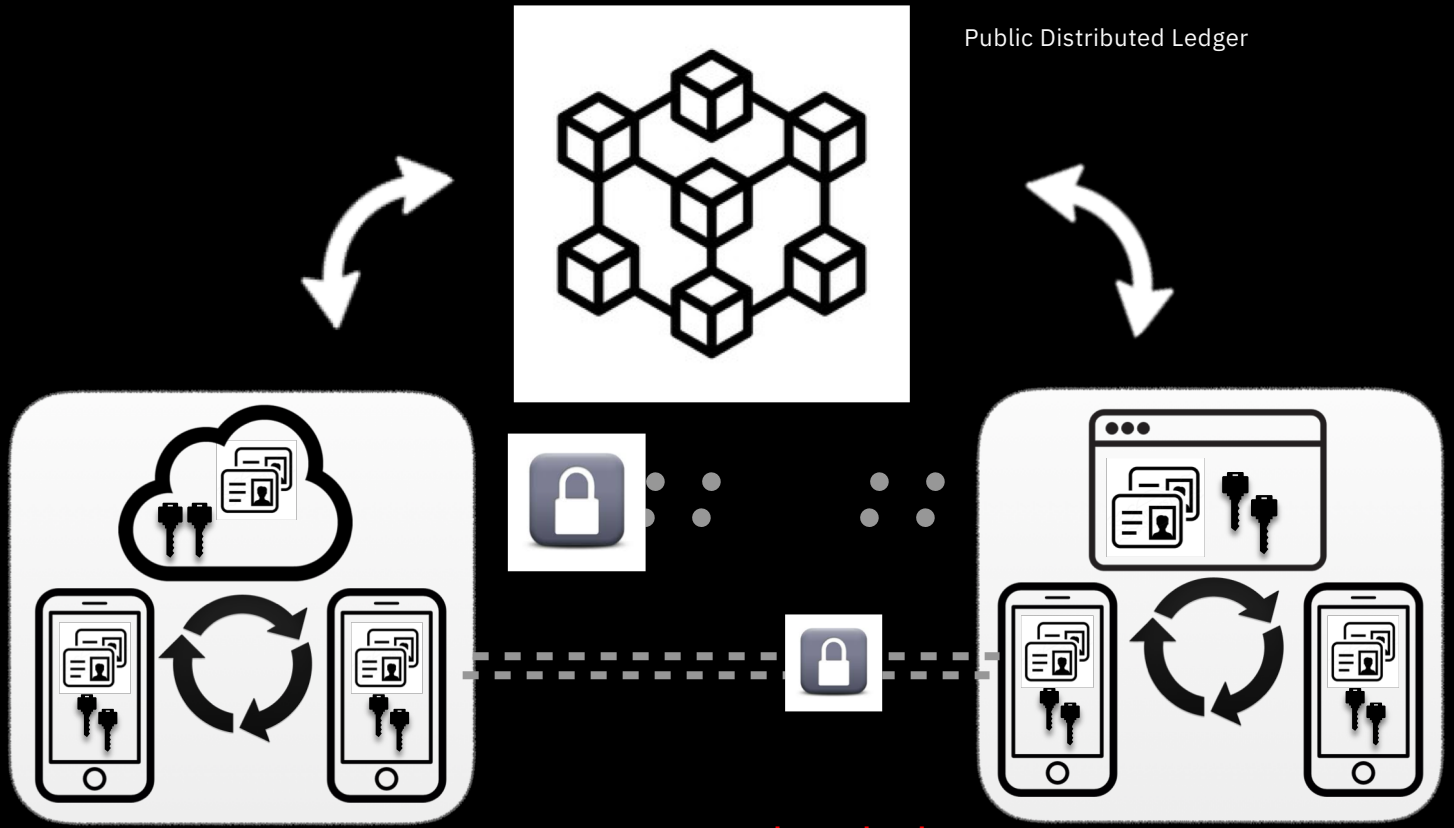
Blockchain provides:

- Immutable recordings of the lifecycle events associated with the binding between a public key and its owner.
- Secure and authentic exchange of keys which was not possible using PKI.

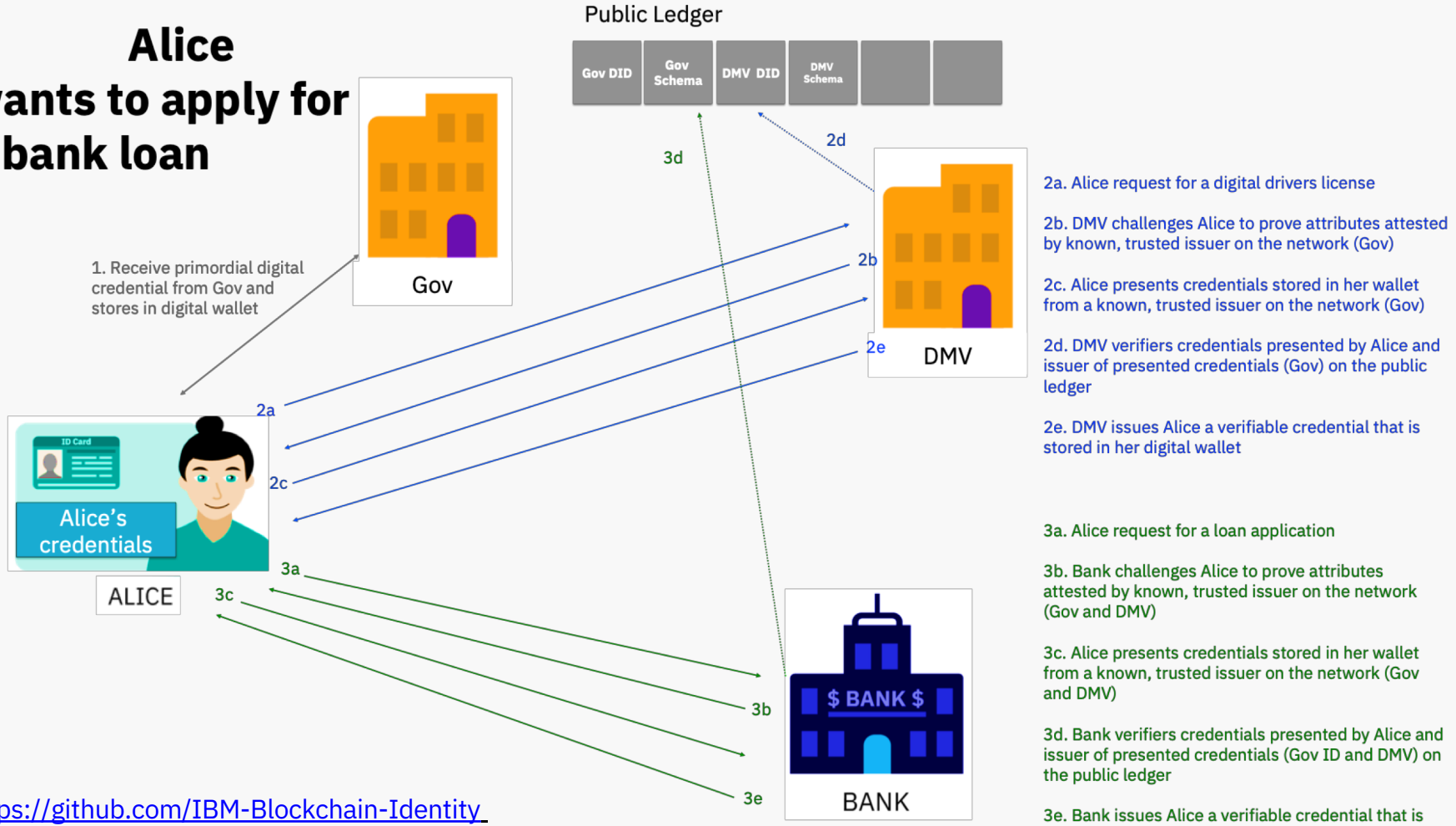
A blockchain ledger is <u>not</u> intended to be used for the storage of PII data.

Peer-to-peer interactions at the edges of the network

P2P network of distributed private agents working in parallel with the distributed ledger.



Alice wants to apply for a bank loan



2a. Alice request for a digital drivers license

2b. DMV challenges Alice to prove attributes attested by known, trusted issuer on the network (Gov)

2c. Alice presents credentials stored in her wallet from a known, trusted issuer on the network (Gov)

2d. DMV verifiers credentials presented by Alice and issuer of presented credentials (Gov) on the public ledger

2e. DMV issues Alice a verifiable credential that is stored in her digital wallet

3a. Alice request for a loan application

3b. Bank challenges Alice to prove attributes attested by known, trusted issuer on the network (Gov and DMV)

3c. Alice presents credentials stored in her wallet from a known, trusted issuer on the network (Gov and DMV)

3d. Bank verifiers credentials presented by Alice and issuer of presented credentials (Gov ID and DMV) on the public ledger

3e. Bank issues Alice a verifiable credential that is stored in her digital wallet for issuing her loan

https://github.com/IBM-Blockchain-Identity
https://www.youtube.com/watch?v=0bAewVLl1TI

Lessons for NFV

What is Responsible Use for NFV?

Bias

Data Privacy

Power Consumption

Bias

Be aware it exists!

Look for instances where people are impacted by AI decisions

Badging in purchased AI models?

Churn Prediction

VALIDATED

Problem Statement:

Anticipating and preventing customer churn is a top priority for telcos, as customer acquisition costs increase. If a company can effectively predict—and prevent—even just 1% of customers from leaving, it can potentially increase profits by a much higher rate.

The data required to predict churn accurately are complex and diverse, ranging from time series data around plan usage to unstructured complaints and support requests. Telcos are increasingly turning to complex machine learning methods to build accurate churn prediction models—but because customer churn is a dynamic problem based on behavior factors, these models can quickly become out of date.

Watson OpenScale Solution:

Telcos invest in developing complex machine learning models to predict churn; however, a churn model that works well today could cease to perform in the future due to changes in customers' behavioral patterns driving churn. Once a good churn model has been developed, validated, and deployed in production, it is susceptible to concept drift, becoming inaccurate over time as customer behavior changes.

Tackling concept drift is an important part of maintaining churn models in production. Watson OpenScale's **runtime monitoring features** allow data scientists and business owners alike to track the accuracy and performance of their models over time, so that they can catch potential drift and retrain their models to maintain effectiveness.

Marketing teams can also mine metrics from OpenScale's **data mart** in order to correlate business outcomes of retention campaigns.

Data Privacy

In business ecosystems, leverage well-constructed blockchains to better protect data

Leverage telcos' reputation for privacy to participate in new revenue offerings

Telcos need to consider four strategic levers for Blockchain

Future Operations

Future Customer Engagement

New Ecosystems

1. Demands for Privacy, Transparency, Trust and Security throughout

Telcos remain amongst the most trusted parties for handling personal data and securing privacy

2. Future of Operations

- Provenance & asset management
- Improve internal cost and efficiencies via smart contract
- Streamline and automate internal business processes
- Increase transaction speed: reduced clearing and settlement time
- Disintermediation opportunities (eg. Financial Clearing House)

3. Future of Customer Engagement

- Improve customer experience (number portability, disputes, etc.)
- New business models, enhancing customer engagement (digital identity, content, mobile money/wallets)
- New trusted & privacy services (Identity As-A-Service)
- Community, socio-economic services

4. Ecosystem Plays

- New business models with shifting profit pools (winner take most)
- Complex transactions with multi-participants, emergence of consortia
- Partnerships & network of networks

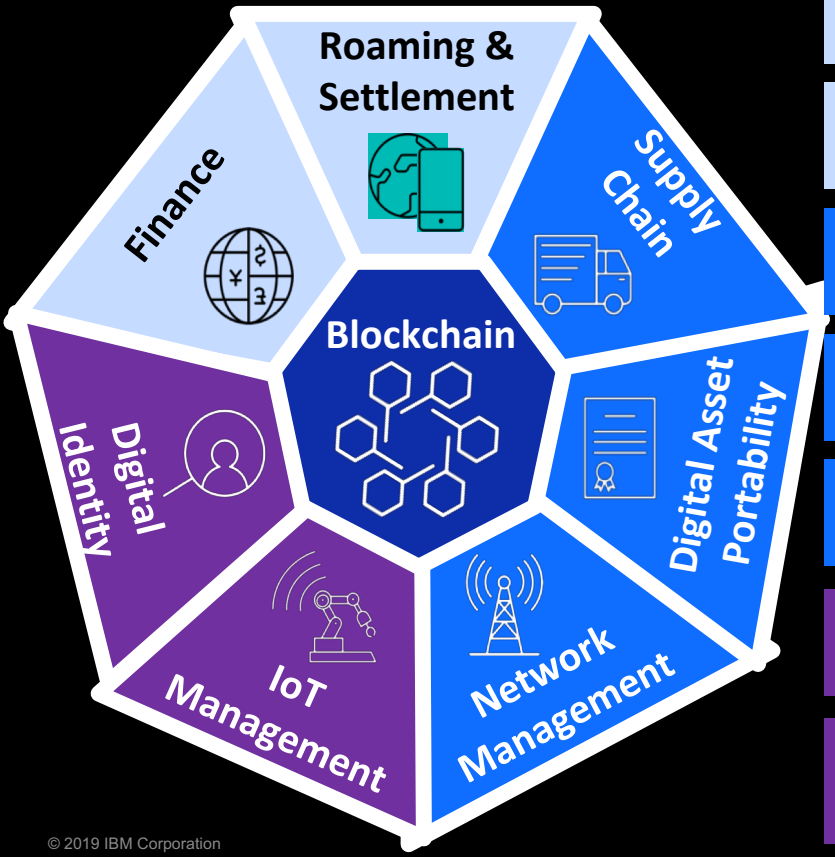
Blockchain-As-A-Service: Digital Service Enablers

$ Thousands

$$ Millions

Exponential Value $$$ billions!

Use cases currently being discussed by TME clients



Finance	• Accounts Payable • Procurement, streamlining the payments & settlement process • Dispute resolutions simplify audit/compliance
Roaming & Settlement	• Roaming settlements, Inter-company settlements • Roaming for IoT • Identify subscriber Fraud and Overage Management.
Supply Chain	• Inventory Management • Supply chain network equipment, devices, components • Supplier, distributors and partner transaction efficiency
Digital Asset Portability	• Mobile/Fixed Number portability across MNO's • Global Data Portability initiative • Do Not Call (DNC) Registry
Network Management	• Acquisition of planning & approvals for network roll out • NFV enhancement: enable virtual devices, send charging data, authentication, authorization and automated provisioning
IoT Management	• eSIM activation tracking and management on IoT platform • Shared ledger smart cities: metered data, payment per use • Alerts and automated actions defined by thresholds
Digital Identity	• Decentralised Identity Management • Identity-As-A-Service • IoT Digital Credentials

Power Consumption

In NFV, power consumption could be a serious issue:

- 5G & Edge are driving distribution of VNFs to locations with minimal control of power sources (i.e. opposite of a large green-energy data center)
- Hardware control & refresh cycles also more labor intensive

Should power consumption of VNFs be considered in purchasing decisions?

Developing Resource Efficient Software

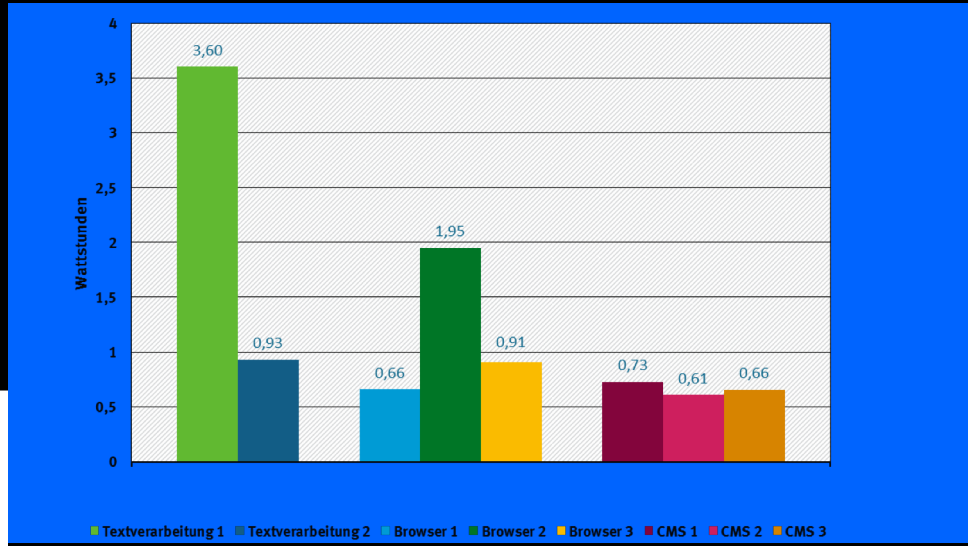
Research Project

- Methods & tooling for measuring hardware utilization and energy consumption
- Evaluation criteria catalog for software
- Recommended criteria for a software eco—label

Table 1: Classification of evaluation criteria

1	Resource efficiency	2	Potential hardware useful life	3	User autonomy
1.1	hardware efficiency	2.1	backward compatibility	3.1	transparency and inter-operability
1.2	energy efficiency	2.2	platform independence and portability	3.2	uninstallability
1.3	resource management	2.3	hardware sufficiency	3.3	maintenance functions
				3.4	independence of out-side resources
				3.5	quality of product in formation

Source: Criteria catalogue for sustainable software, see Anhang 1



Entwicklung und Anwendung von Bewertungsgrundlagen für ressourceneffiziente Software unter Berücksichtigung bestehender Methodik

von

Dipl.-Ing. Jens Gröger, Dr. Andreas Köhler Öko-Institut e.V., Freiburg
Prof. Dr. Stefan Naumann, Andreas Filler, M.Sc., Achim Guldner, M.Sc., Eva Kern, M.Sc.
Institut für Softwaresysteme, Hochschule Trier, Umwelt-Campus Birkenfeld
Prof. Dr. Lorenz M. Hilty, Yuliyan Maksimov, M.Sc. Forschungsgruppe Informatik und Nachhaltigkeit, Universität Zürich

What are your ideas for responsible use of NFV?

Thanks!

Rachel K. E. Bellamy -- Principal Research Staff Member; IBM Research AI

Susan Malaika -- Open Tech for Data & AI; IBM Cognitive Applications

Utpal Mangla--VP & Partner, Watson AI, Blockchain Leader; IBM GBS

Milan Patel -- Offering Mgr, Blockchain Trusted Identity; IBM Industry Platform

Christopher Ferris -- Distinguished Engineer; IBM Cognitive Applications

Adam Cutler -- Distinguished Designer; IBM Cloud and Cognitive Software

Daniela Barbosa -- VP of World Wide Alliances, Hyperledger

Jens Gröger -- Senior Researcher, Öko-Institut e.V.

AIFairness 360 Research:

Rachel K. E. Bellamy [1] Kuntal Dey [2] Michael Hind [1] Samuel C. Hoffman [1] Stephanie Houde [1]
Kalapriya Kannan [3] Pranay Lohia [3] Jacquelyn Martino [1] Sameep Mehta [3] Aleksandra Mojsilovic [1]
Seema Nagar [3] Karthikeyan Natesan Ramamurthy [1] John Richards [1] Diptikalyan Saha [3] Prasanna Sattigeri [1]
Moninder Singh [1] Kush R. Varshney [1] Yunfeng Zhang [1]