



# Bitcoin, Blockchains and Efficient Distributed Spacecraft Mission Control

Dan Mandl Code 581  
GSFC IS&T Colloquium  
9-13-17



# Cryptocurrency Basics

- Store value
- Build ecosystem to enable efficient distribution and management of value
  - ✓ **Original Blockchain Organizations:** Bitcoin, Litecoin, Ethereum, primarily interested in maintaining the base infrastructure that keeps the blockchain operating as is (or part of a roadmap). Primarily focused on the infrastructure necessary for the cryptocurrency operating smoothly
  - ✓ **Decentralized Services on Top of Blockchain** - e.g Cosmos – an Internet of blockchains, Swarm – decentralized crowdfunding, Storj – distributed encrypted blockchain based , open source, cloud storage, or blockchain stacks using multiple blockchain services
  - ✓ **Enterprise Blockchain Organizations** -These include organizations like Ripple, Ethereum Enterprise Alliance and Hyperledger.
    - Purpose is to take public blockchain technology and figure out how to make it 'work' for current enterprise organizations.
    - While some goals are in alignment with the public blockchain goals, specific use cases will turn enterprise blockchain into a classification of its own. This means we need to consider the Enterprise use cases as separate entities



# Cryptocurrency Basics



## ✓ Entrepreneurial Ventures utilizing Blockchain

- These are start-ups and businesses not focused on infrastructure, but building services to utilize blockchain technology.
- Current exchanges (such as Coinbase) as well as companies working inside Consensys would be an example of this (check out VariabL, a Decentralized Options Market). These are guys that are building services outside of the blockchain to make it more useful.
- As time goes on, this group will grow dramatically as the underlying technology gets more mature.
- Blockchain to manage space applications
  - ✓ Value is services capacity e.g. downlink capacity, imaging capacity, power capacity, ground networks for distribution etc
  - ✓ any limited resource

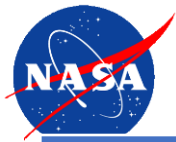
Source: <https://www.quora.com/As-of-early-2017-what-is-a-summary-of-the-cryptocurrency-ecosystem>



# Cryptocurrency Recent News



- As of September 6, 2017, cryptocurrency market capitalization was \$157 billion compared to \$12 billion Sept 12, 2016 (source: <https://coinmarketcap.com/charts/>)
- Trading volume for all cryptocurrencies was recently \$5 - \$9 billion USD per 24 hour period versus \$112 million Sept 12, 2016 (source: <https://coinmarketcap.com/charts/>)
- Market capitalization climbed 17% from Sept 5, 2017, \$20 billion in 24 hours, recovering from 25% decline earlier in week
  - ✓ China's financial regulators deemed illegal, initial coin offerings (ICO), or sale of new cryptocurrencies to fund blockchain project development
- Van Eck (24.7 billion money manager) filed with SEC to start an ETF based on Bitcoin linked derivatives on Aug 11, 2017 (going more mainstream)
- Previously SEC shot down Cameron and Tyler Winklevoss' (Facebook, ConnectU) request for a bitcoin ETF listing on Bats, the stock exchange recently purchased by exchange giant CBOE Holdings, in March.



# Five of Top Crypto-Currencies



Crypto	Key Functions	Basic Unit	% market Sept 12, 2016	% market Sept 12, 2017	% price increase since 1/1/2017	Comment
Bitcoin	Public blockchain, P2P transactions	bitcoin	80	47.5	451 (520 max approx.)	85% of market as recently as Mar 5, 2017
Ethereum	Smart Contracts	ether	8.22	19.08	3871 (5000 max)	
Neo	Chinese version of Ethereum	neo	0	0.72	15753 (33340 max)	
Litecoin	Faster transactions and improved storage requirements	Litoshi	1.5	2.38	1438 (1856 max)	
Ripple	Commercial Blockchain, speed, private P2P	XRP/drops	1.72	5.6	3505 (5960 max)	

Source: <https://coinmarketcap.com/charts/>

Daniel Mandl Code 581 NASA/GSFC

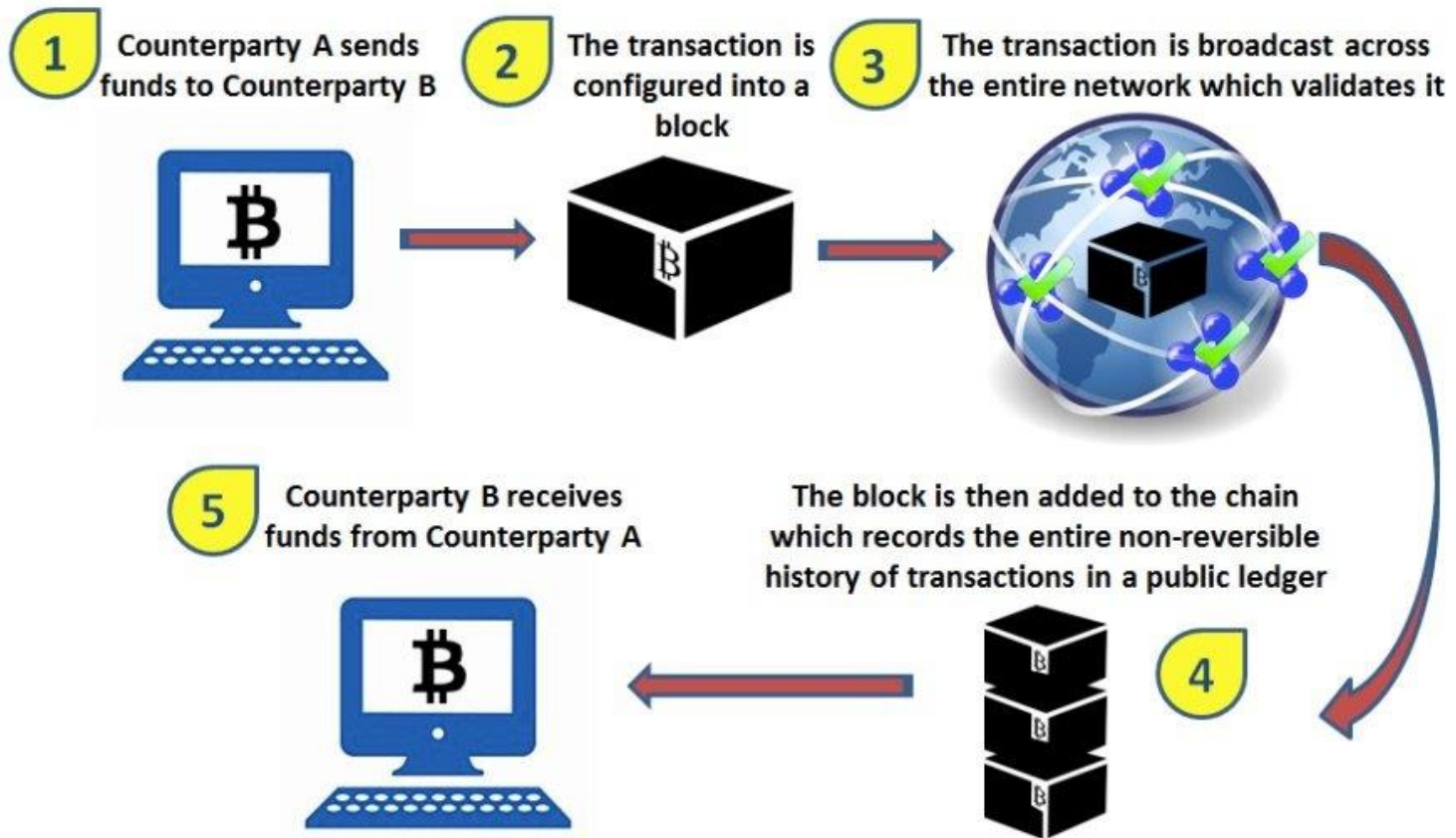


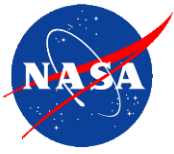
# Distributed Spacecraft Mission Definition

- A Distributed Spacecraft Mission (DSM) is one that involves multiple spacecrafts to achieve one or more common goals.
- If defined from inception, then it is called a “constellation”
- If it becomes a DSM after the fact, then it is called an “ad hoc” DSM or “virtual mission”

from GSFC internal report by Jacqueline LeMoigne

**Exhibit 1: The Blockchain is a distributed, public ledger, most commonly known as the core underlying technology for Bitcoin**





# Key Bitcoin Characteristics



- Distributed ledger (stored in blockchain)
- Easy to set up and participate (low entry barrier)
- Anonymous (public access)
- Transparent, holographic, provenance, audit trail, trust, collaboration
- Minimizes transaction fees (very low cost)
- Fast (payments arrive in minutes) versus international banking delays
- Non-repudiable, immutable, encrypted





# Benefits for DSM Use



- Lowers cost
- Increases reliability
- Reduces cost to join constellation since all that is needed is blockchain interface (similar to automotive Onboard Diagnostics (OBD II) standards)
- Automatic audit trail
  - ✓ Provides data provenance
  - ✓ Great tool for debugging (similar to automotive Onboard Diagnostics (OBD II) standards)
  - ✓ Provide data for artificial intelligence tools
    - ❖ More and easy access to training data
    - ❖ Enables continuous learning because new data immediately and constantly comes in (perfect for Deep Learning/Tensor Flow)
  - ✓ Can document digital rights and therefore promotes sharing of data
    - ❖ People are willing to share their data in open space if data is protected and if Intellectual Property rights protected
  - ✓ Makes testing easier
- Enables easier and more automation at lower cost
  - Automatic resource outage alerts
  - Enables localized automated replanning (e.g. ground station out, replan for later downlink without ground as central coordination point, thus less efficient)
  - Enables constellation level model-based diagnostic tool similar to Livingstone created by Ames and run onboard Earth Observing 1 (also similar to OBD II but for constellations)



# Problems to Solve for DSM Use



- Standard blockchains used for Bitcoin are slow
  - ✓ Transactions validated in blocks every 10 minutes
- Blockchain file sizes are very large and the initial download can take 24-48 hours on Bitcoin
- Concurrency issues
- Need light, hardened version similar to what was done for the Core Flight Software package to use on spacecrafts



# Private Blockchain (Ripple and others)



- Limited user base
- Users need permission
- Transactions verification different – centralized verification system
- Faster
- More efficient with data storage
- Augmented with commercial distributed databases to enhance performance



# Ledgers



CODES - ACH: ACH Payment | ATM: Cash Withdrawal | BP: Bill Payment | DC: Debit Card | DD: Direct Deposit | SF: Service Fee | WT: Wire Transfer

CHECK NUMBER/CODE	DATE	TRANSACTION DESCRIPTION	PAYMENT/DEBIT	DEPOSIT/DEBIT	BALANCE
	5/1/15	Starting Balance			140 00
314	5/1/15	XYZ Electric Company	80 00		-80 00
					60 00
DD	5/1/15	ABC Employer		1,500 00	+1500 00
					1,560 00
315	5/3/15	Jane Doe	30 00		-30 00
					1,530 00
BP	5/5/15	Netflix	10 00		-10 00
DC	5/6/15	123 Grocery Store	85 00		

- Example of checkbook ledger where someone keeps track of their spending transactions
- Key issue: checks validated and cleared

- Example of EO-1 Activity Plan which kept track of operation activities and acted as localized ledger
- Key issue: Interim and End-Item verification (partial list)
  - Did image goals get uploaded
  - Did image get taken
  - Did image data get downlinked to ground station
  - Did ground station successfully receive downlink and forward
  - Did Data Processing System successfully process to Lev0, Lev1
  - Did image get published or sent to user

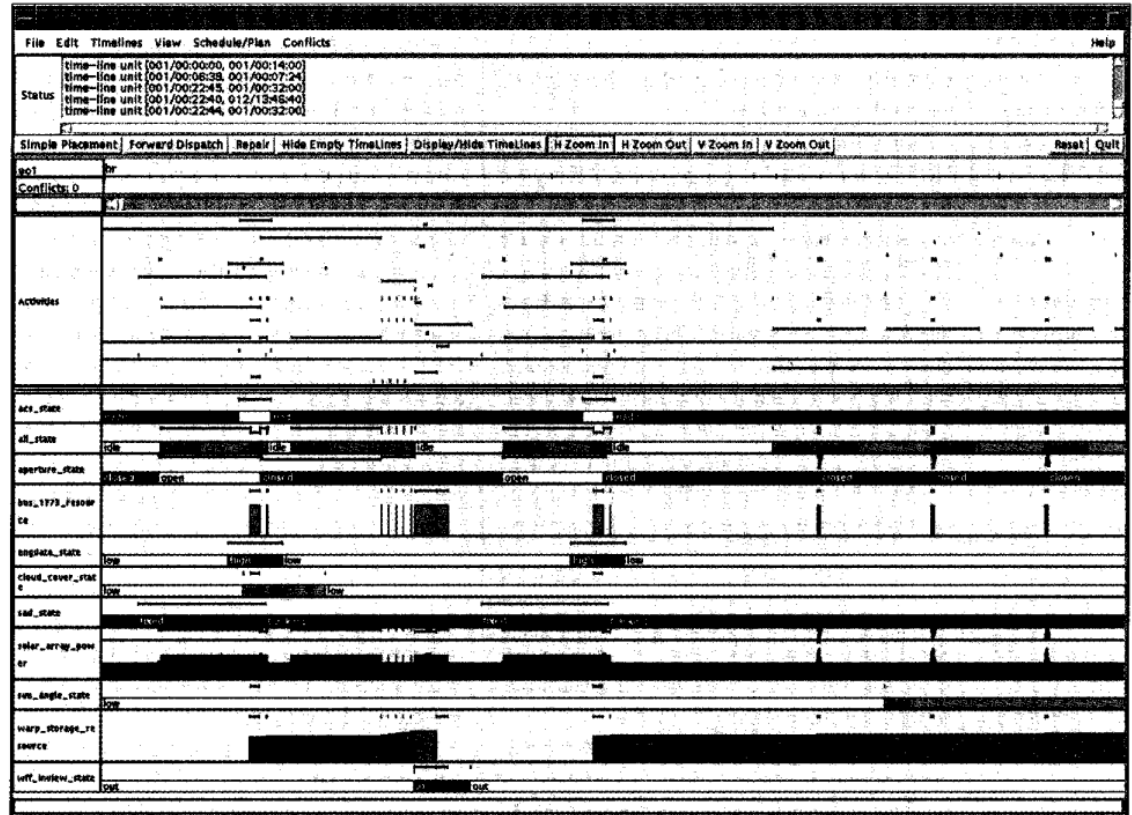
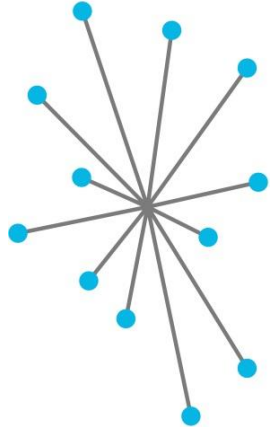


Figure 1. A one-week operations plan for the New Millennium Earth Orbiter One generated by the Aspen planning system.

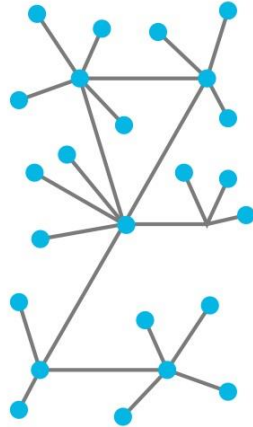


# Different Ledger Configurations *Goddard* SPACE FLIGHT CENTER

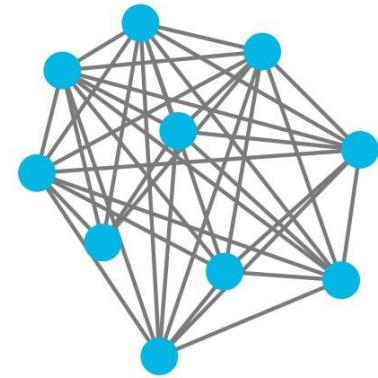
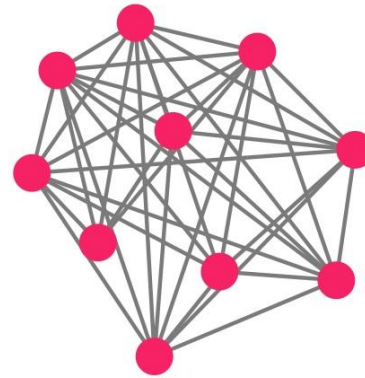
## Centralized



## Decentralized



## Distributed Ledgers



## The New Networks

Distributed ledgers can be public or private and vary in their structure and size.

Public blockchains

Require computer processing power to confirm transactions ("mining")

- Users (●) are anonymous
- Each user has a copy of the ledger and participates in confirming transactions independently

- Users (●) are not anonymous
- Permission is required for users to have a copy of the ledger and participate in confirming transactions



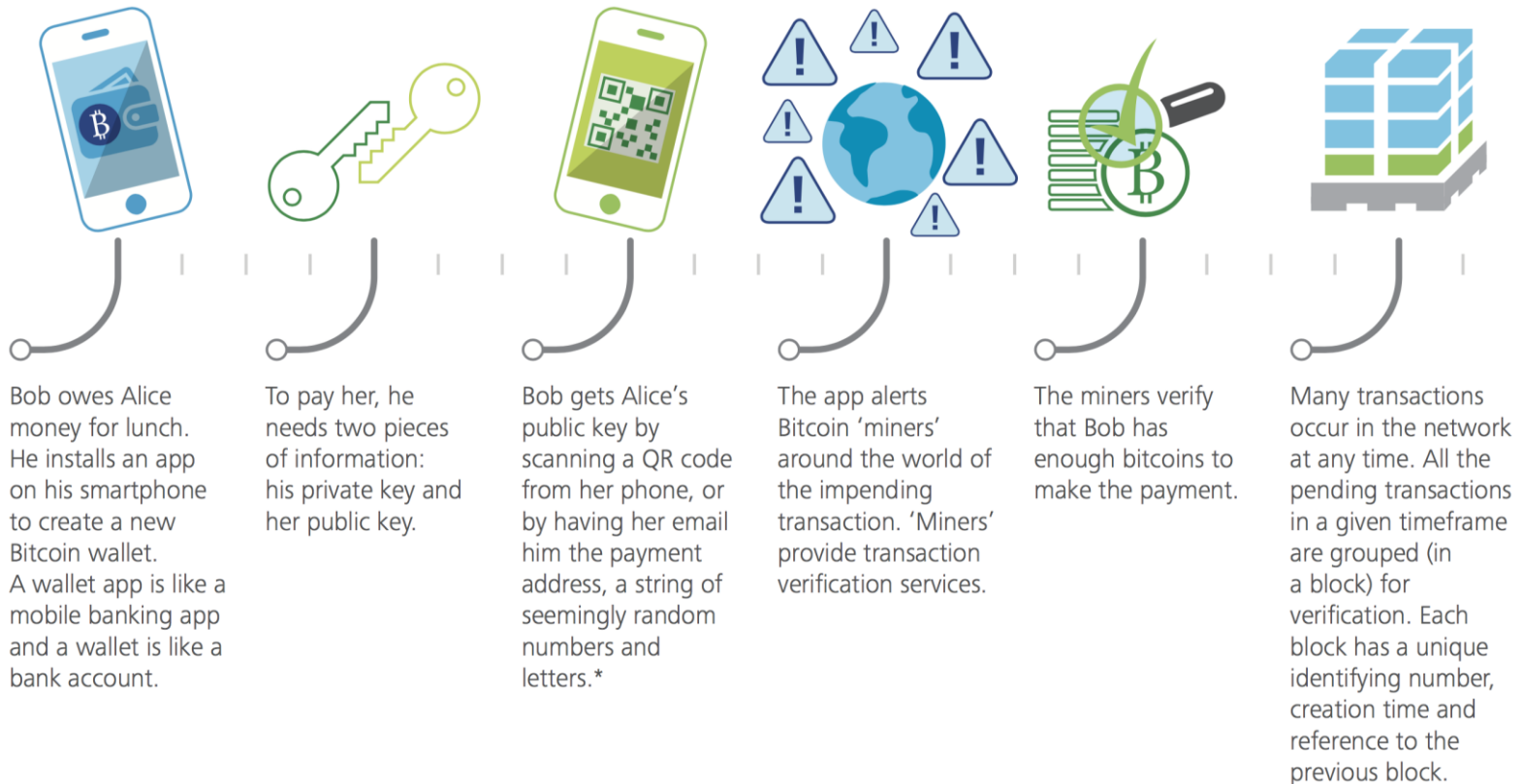
Most if not all spacecraft operations live here



# Some Details

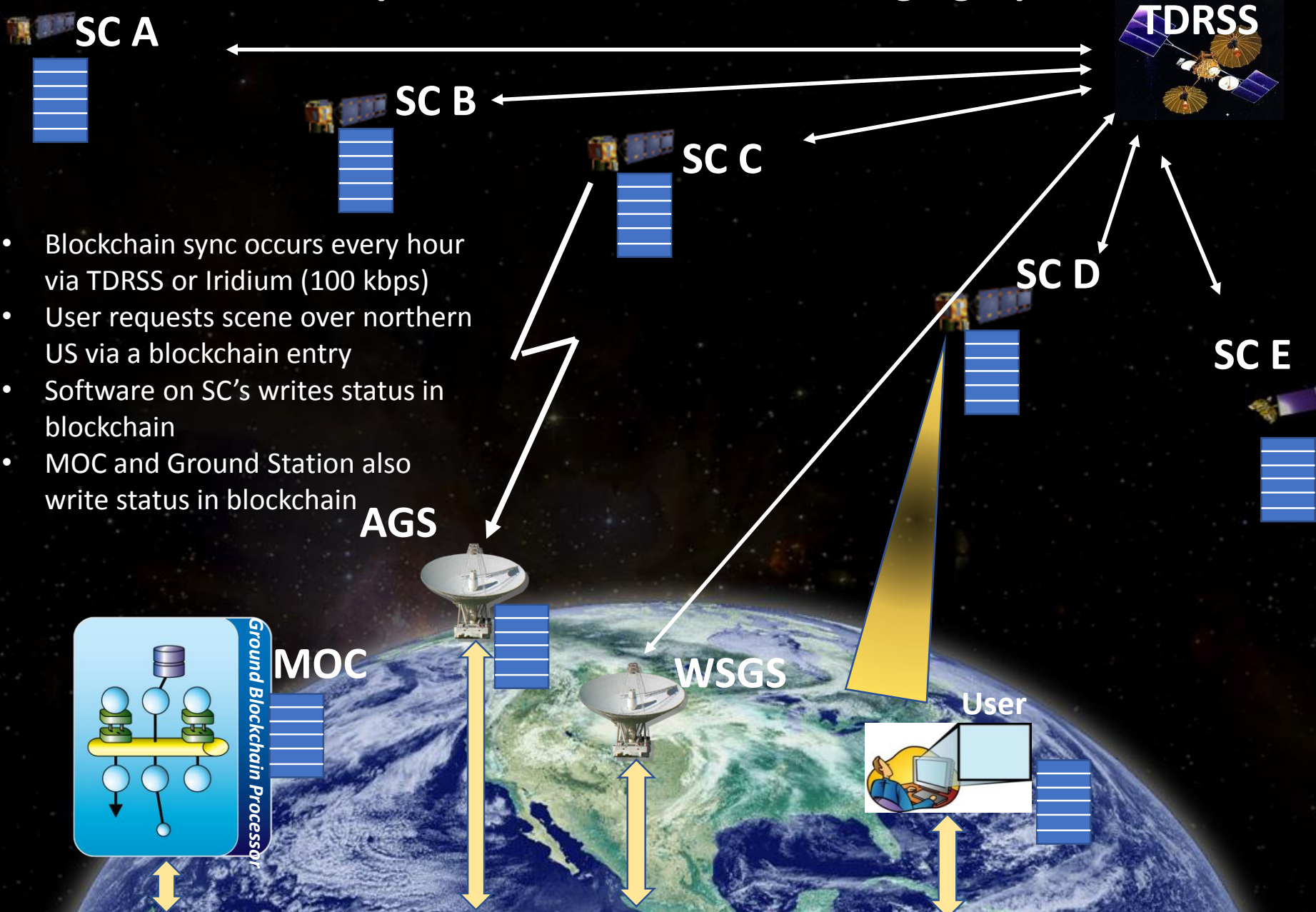


Figure 1. How the Bitcoin blockchain works



\*Anyone who has a public key can send money to a Bitcoin address, but only a signature generated by the private key can release money from it.  
Graphic: Deloitte University Press. Source: American Banker<sup>20</sup>

# Blockchain in Space Scenario 1 – Basic Imaging Operations



- Blockchain sync occurs every hour via TDRSS or Iridium (100 kbps)
- User requests scene over northern US via a blockchain entry
- Software on SC's writes status in blockchain
- MOC and Ground Station also write status in blockchain

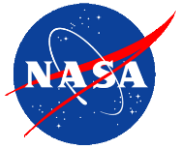


# Basic Imaging Operations



- User enters image request, location and timeframe via blockchain entry
- Assets provide availability which includes overflight times, inview times for ground stations and prescheduled conflicts
- First available asset schedules image time and downlink time as needed
- Operation errors, outages etc. are recorded on blockchain
- Completion time, downlink time to ground station and successful publishing of data to user specified location are documented in blockchain.





# Smart Contracts (Ethereum and others)



- Autonomous
- Encryption allows safeguarding of documents
- Documents are backed up since many copies
- Low cost to execute since no intermediary
- Accurate because terms are executed via software directly from contract



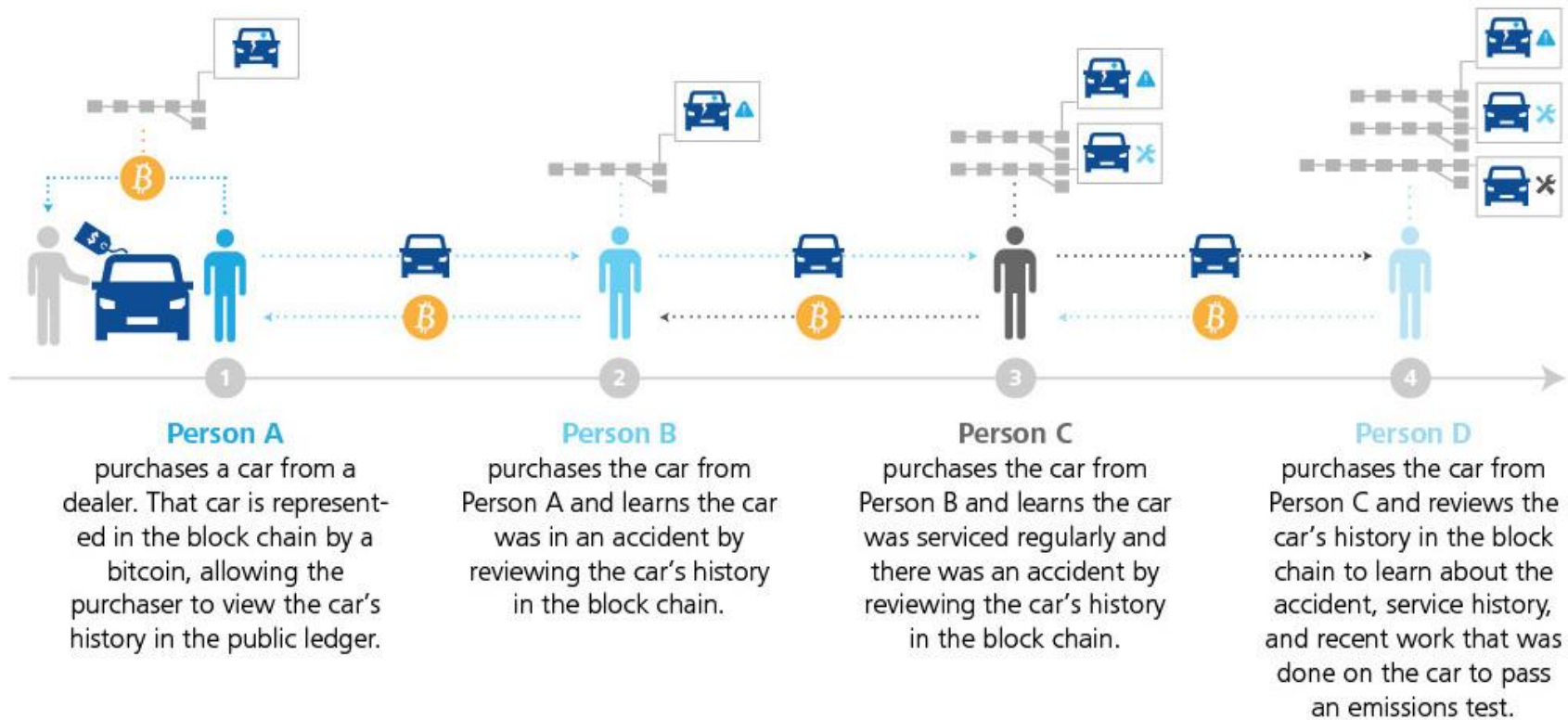
# Porting Operational Spacecraft Software to Distributed Smart Contracts



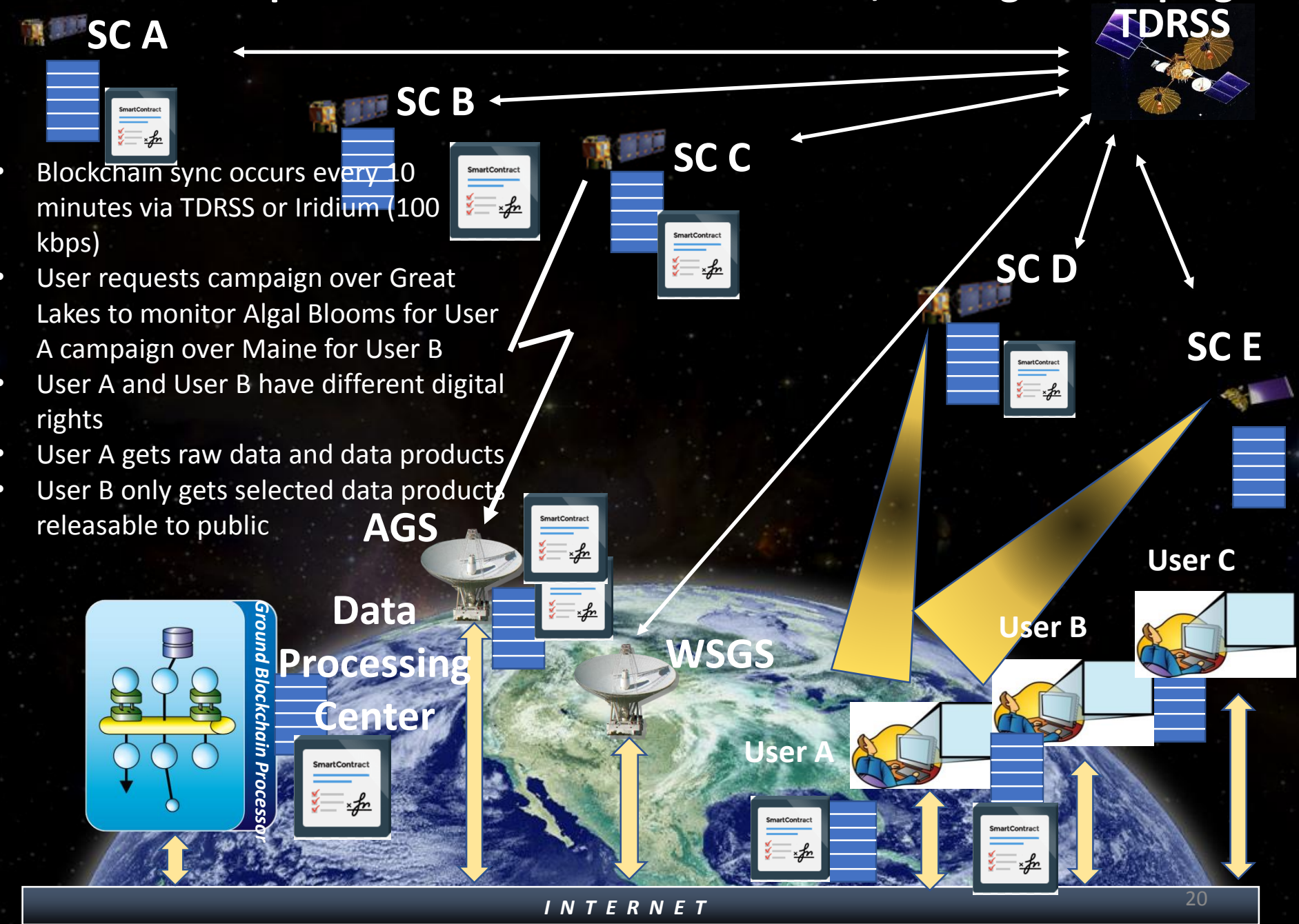
- Autonomous Spacecraft Experiment (ASE) – onboard autonomy that ran on Earth Observing 1 (EO-1) for 12 years
- Livingstone Model-Based Onboard Diagnostic tool – ran on EO-1
- AMPS, ASPEN and other planning tools
- Augment all of the SensorWeb tools (<https://sensorweb.nasa.gov>)
- Accurate because terms are executed via software directly from contract



# Smart Contract Example



# Blockchain in Space Scenario 2 – Smart Contract, Managed Campaigns



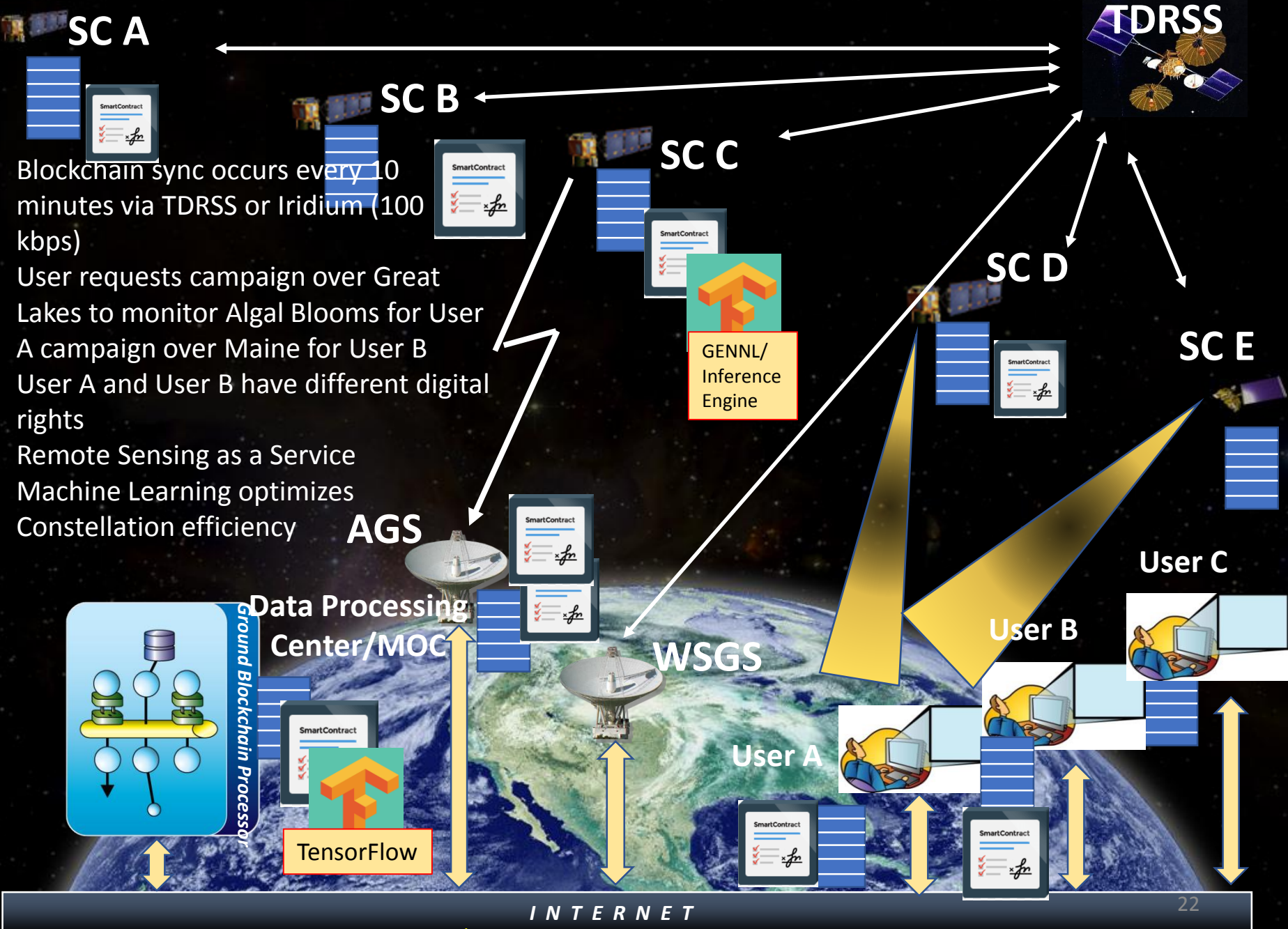
- Blockchain sync occurs every 10 minutes via TDRSS or Iridium (100 kbps)
- User requests campaign over Great Lakes to monitor Algal Blooms for User A campaign over Maine for User B
- User A and User B have different digital rights
- User A gets raw data and data products
- User B only gets selected data products releasable to public



# Smart Contracts and Managed Campaigns

- Users submit smart contract to complete a series of images with conditions (e.g. weekly diurnal over a growing season spectral measurements to create time series)
- Assets self-schedule and route data and data products according to users depending on data rights
- Users provide backup imaging plans when assets are out of commission or failures occur
- Users provide time constraints and locations desired
- Audit trail of completed imaging operations with successes and failures documented in blockchain

# Blockchain in Space Scenario 2 – Smart Contract, Machine Learning



- Blockchain sync occurs every 10 minutes via TDRSS or Iridium (100 kbps)
- User requests campaign over Great Lakes to monitor Algal Blooms for User A campaign over Maine for User B
- User A and User B have different digital rights
- Remote Sensing as a Service
- Machine Learning optimizes Constellation efficiency



# Smart Contracts, Machine Learning to Optimize Constellation



- Users submit smart contract to complete a series of images with conditions (e.g. weekly diurnal over a growing season spectral measurements to create time series)
- Assets self-schedule and route data and data products according to users depending on data rights
- Machine learning allocated Constellation resources based on learned methods to optimize image output and minimize cost to user
- Users provide time constraints and locations desired
- Audit trail of completed imaging operations with successes and failures documented in blockchain
- Machine learning uses audit trail to continuously learn and improve
  - E.g Experiment being conducted (Ichoku, Mackinnon, Mandl et al) to observe fires and recognize their radiative type from any angle similar to recognizing a face at any angle



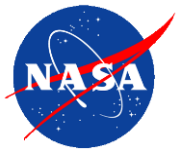
# Blockchains for Artificial Intelligence

- Decentralized and Shared control encouraging data sharing
  - More data and better models
  - Qualitatively new data and therefore qualitatively new models
  - Shared control of AI training data and training models
- Immutability/audit trail
  - Leads to provenance on training/testing data and models to improve the trustworthiness of the data and models
- Native assets/exchanges
  - Leads to **training/testing data & models as intellectual property (IP) assets**, which leads to **decentralized data & model exchanges**. It also gives better control for upstream usage of your data

From: Blockchains for Artificial Intelligence

<https://blog.bigchaindb.com/blockchains-for-artificial-intelligence-ec63b0284984>





# Application Areas for Earth Science

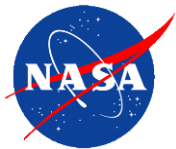
- Low latency operational coordination and dynamic tasking
  - Permission private block chain
  - Support SensorWeb with reduced decision latency
  - Coordinate action without exposing to risk of corruption
- Science mission coordination in Sensor Webs
  - Platforms within SensorWeb shared across diverse set of scientific missions
  - Private ledger will schedule for the various teams and have assurance of identify, access and prevent disruptive use of the instrument
- Distributed Data and Analysis
  - Portions and copies of particular datasets scattered across public and private cloud computing environment
  - Provide record of location
  - Grant and revoke access permissions
  - Provide record of derived data
- Citizen Science
  - Collaborative access to science data
- Management of the Commons
  - Community aligns on a shared interest but cannot establish reciprocal trust between member
  - E.g. Avoiding orbital collisions

Source: AIST Blockchain Study for NASA HQ

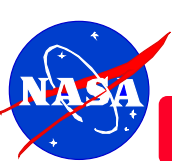


# Related Issues to Blockchain in Space

- Delay Tolerant Network (DTN)
- Consultative Committee for Space Data Systems (CCSDS)



# BACKUP

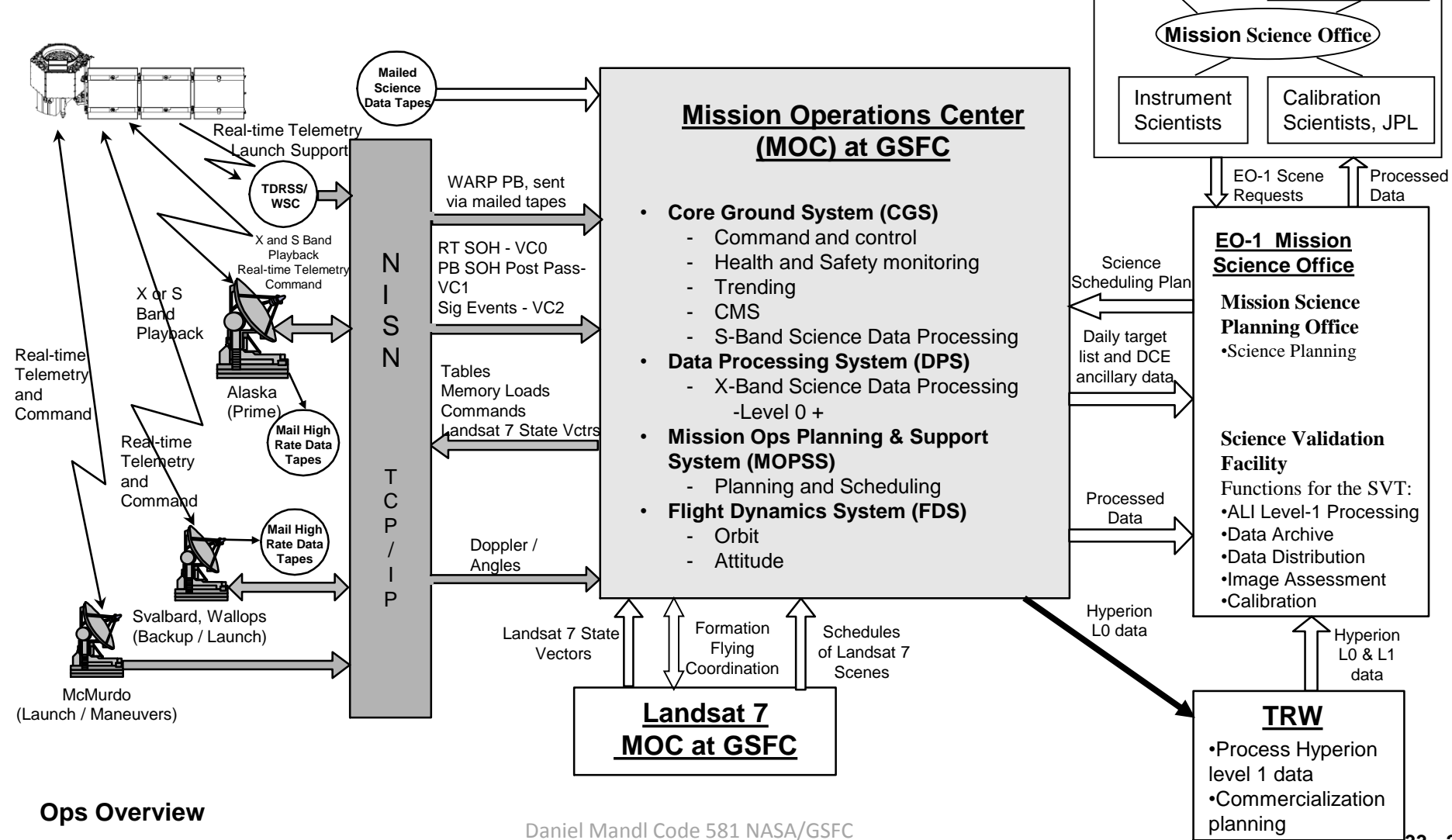


# It's Complicated—Lot's of systems, pipes and delays!

## NMP EO-1

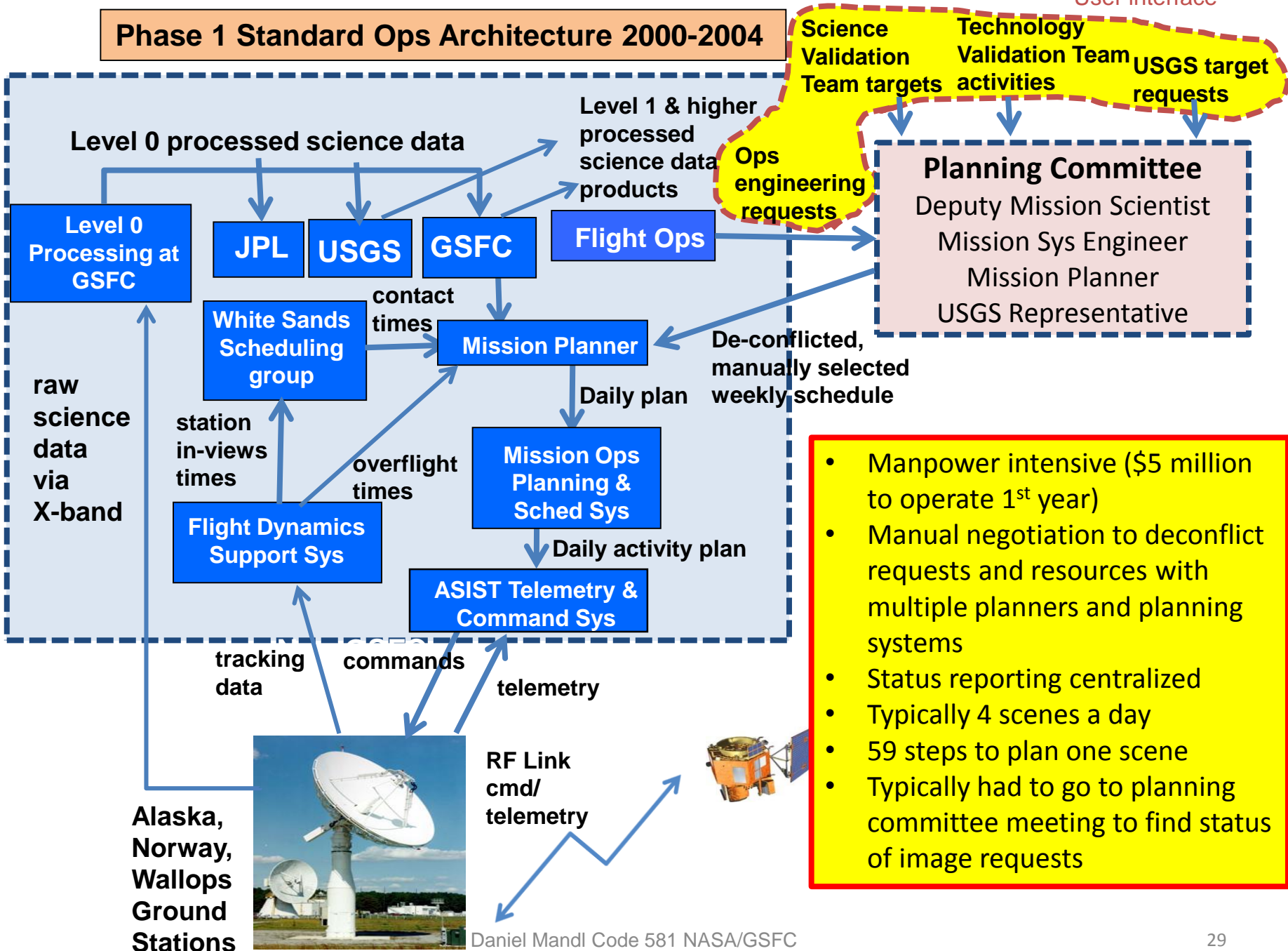
## RED TEAM REVIEW

### Original EO-1 Operations Overview



# Phase 1 Standard Ops Architecture 2000-2004

User interface



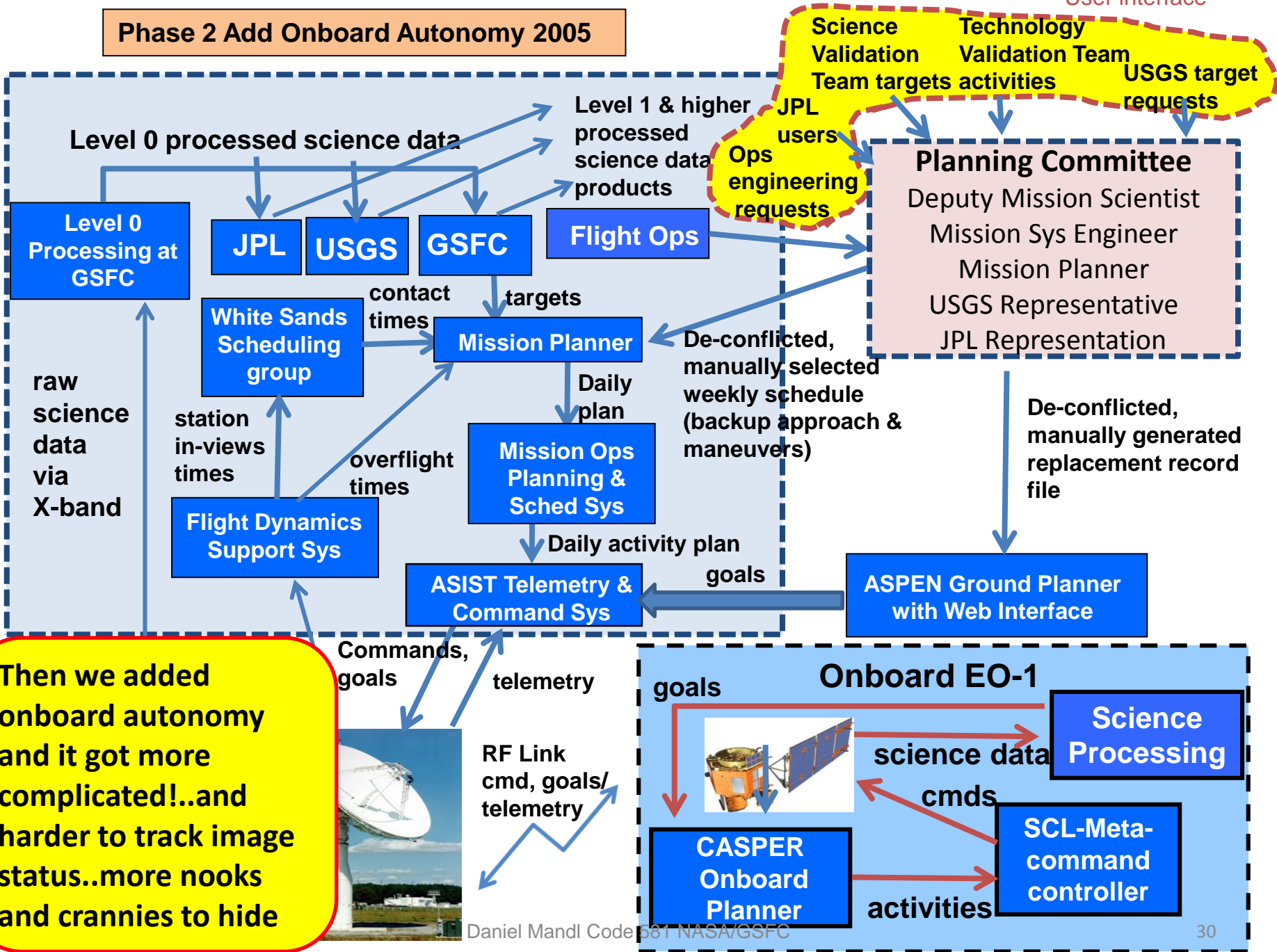
- Manpower intensive (\$5 million to operate 1<sup>st</sup> year)
- Manual negotiation to deconflict requests and resources with multiple planners and planning systems
- Status reporting centralized
- Typically 4 scenes a day
- 59 steps to plan one scene
- Typically had to go to planning committee meeting to find status of image requests

Alaska, Norway, Wallops Ground Stations

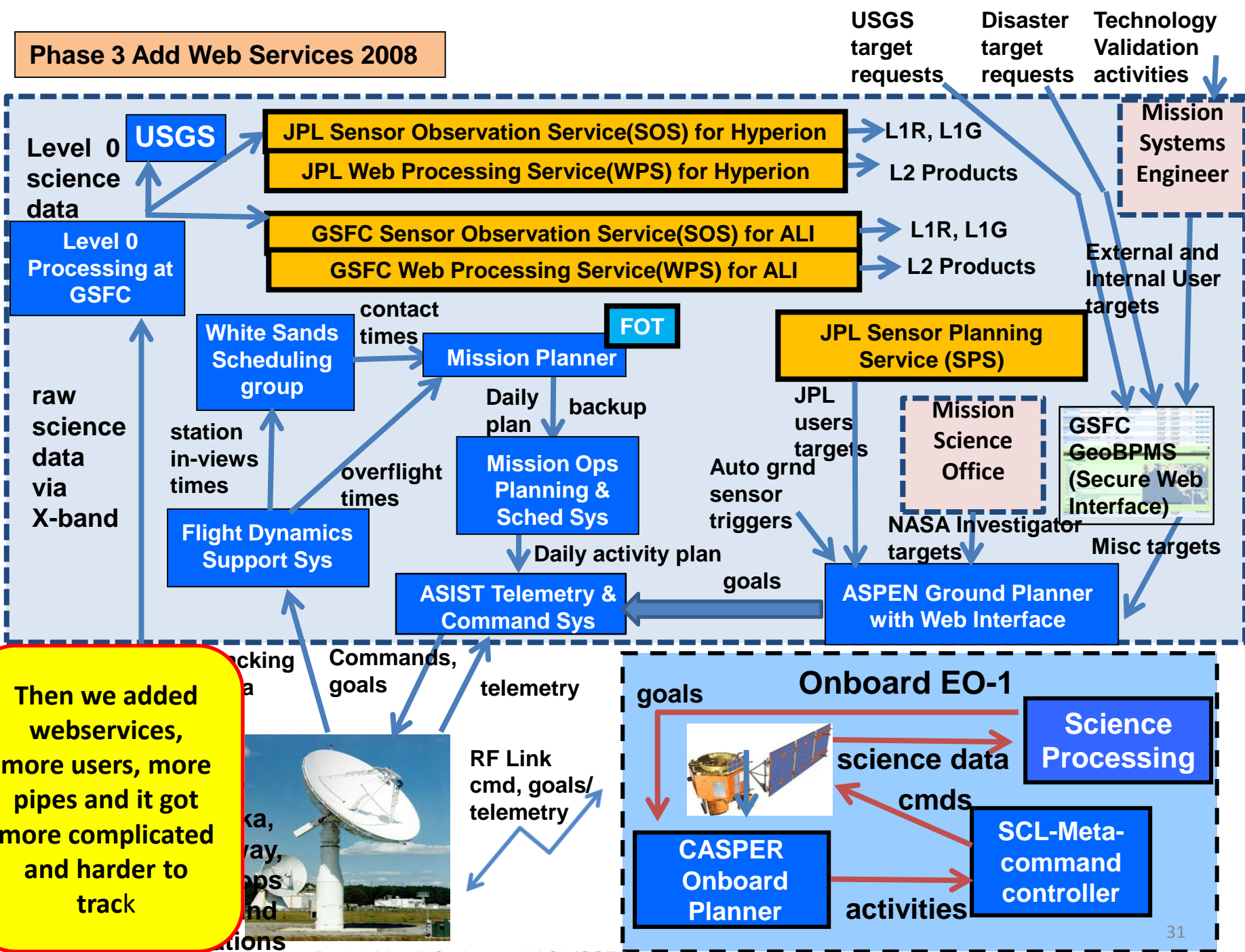


**Phase 2 Add Onboard Autonomy 2005**

User interface



**Phase 3 Add Web Services 2008**



Then we added webservices, more users, more pipes and it got more complicated and harder to track



# Built SensorWeb Tool - GeoBPMS-to Handle Complexity with Automated Web Notification and Tracking

## Direct Internet Access to Data and Tasking

NorthCal Fires	Northern California Fires	fire	patrice	Yosemite Telegraph Fire, Basin Complex, Whiskeytown Complex, ...	06/29/2008 02:13 PM	06/29/2008 09:18 PM	0.4	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Show</a>
NSP	Nationa Signature Program	intel	patrice	TA-03, TA-02, TA-01	03/03/2008 10:25 AM	05/16/2008 12:42 PM	0.2	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Show</a>
Oceans Innovation	Oceans Innovation Workshop Demo	algae	patrice	Monterey Bay	09/10/2008 06:18 PM	09/16/2008 06:38 PM	1.0	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Show</a>
Salt Marshes	To determine salinity contents of flooded areas	flooding	patrice	Lancaster, VA	07/26/2008 02:36 PM	07/26/2008 02:36 PM	-	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Show</a>
SoCal Fires	Southern California Fires	fire	patrice	-	09/06/2007 12:00 AM	06/28/2008 09:23 PM	0.0	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Show</a>
UAV	NASA Ames Ihkana flight scenario	fire	veri_pat	Flood	09/06/2007 12:00 AM	06/04/2008 02:00 PM	0.0	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Show</a>
UAV 2	NASA Ames Ihkana Flight Scenario	fire	scott	UAV 2 Test	09/17/2008 12:40 AM	09/17/2008 12:40 AM	-	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Show</a>
UAV 3	-	fire	UNKNOWN	California	09/18/2008	09/18/2008 03:53 PM	-	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Show</a>

<http://geobpms.geobliki.com/>

Scenario/Campaign Tasking Requests for UAV 3

[Search](#) [Create New](#)

Title	Content	Geolocation	Scenario Feasibilities
<p><b>Tasking Request:</b></p> <p>Title: California</p> <p>Description:</p> <p>Category:</p> <p>Latitude: 41.3</p> <p>Longitude: -123.8</p> <p>Country Code: US</p> <p>Country Name: United States</p> <p>Zone Number: 36</p> <p>Zone Name: Northern California</p> <p>Region Number: 3</p> <p>Region Name: Oregon, California and Nevada</p> <p>Admin Code: CA</p> <p>Admin Name: California</p> <p>Nearby: Notchko, Surgone, Shregegon (historical), Mettah, Pekwan (historical), Pecwan, Johnsons, Waseck, Wright Place, Martins Ferry (historical)</p> <p>Created At: Fri, 19 Sep 2008 02:32:22 -0000</p> <p>Updated At: 2008-09-19</p> <p><a href="#">Show Map</a></p>			
<p><b>Feasibilities</b></p>			

**GeoBliki User Interface**

1 Found

USAFRICOM	USAFRICOM Testing	flooding	cappelaere	Zimbabwe	06/19/2008 02:58 PM	06/19/2008 02:58 PM	-	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Show</a>
-----------	-------------------	----------	------------	----------	---------------------	---------------------	---	--

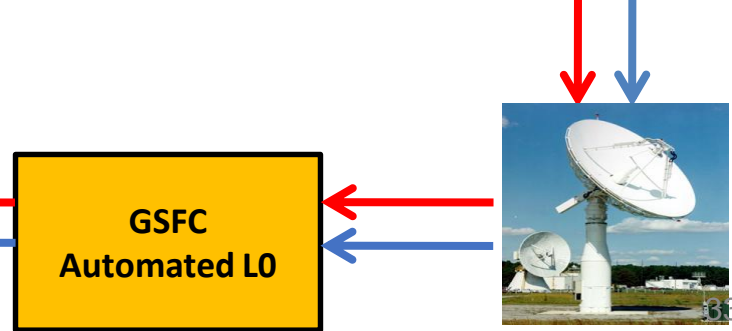
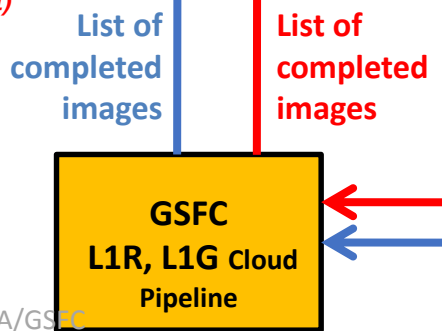
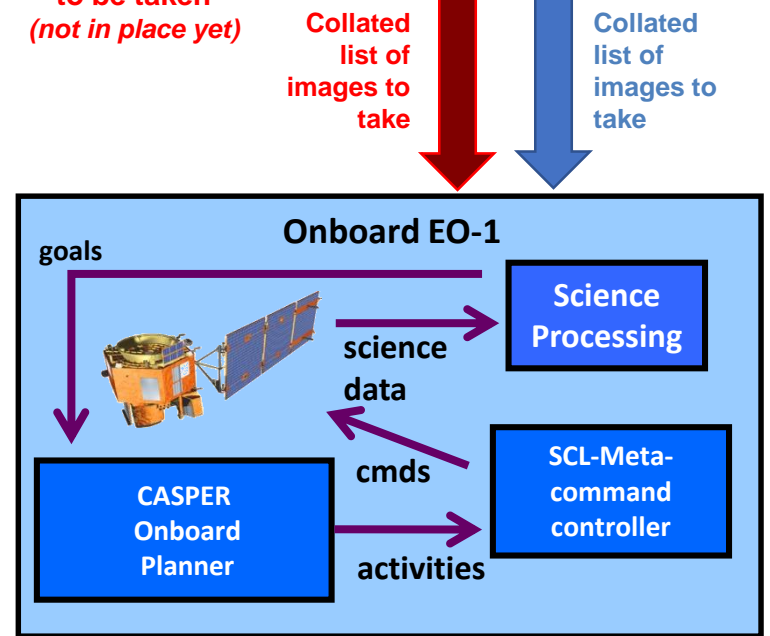
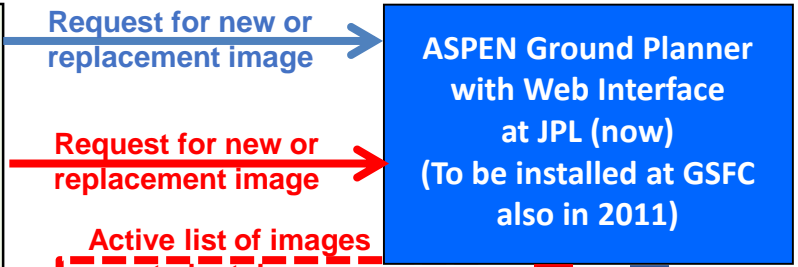
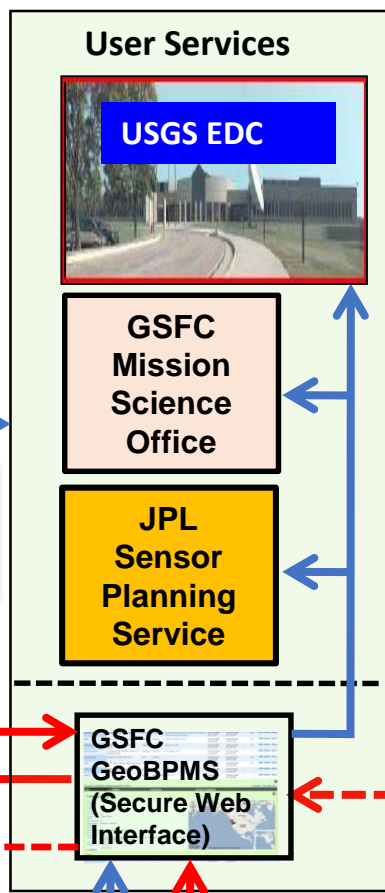
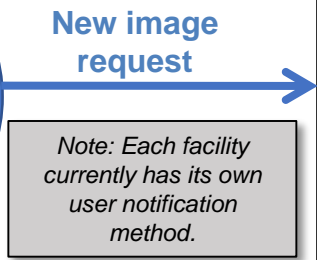
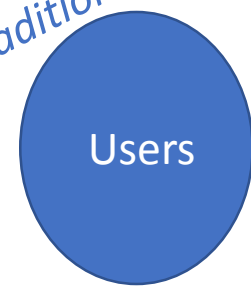


# Problem was that there were too many Legacy Pipes and it took a while to cobble custom notification alerts from various systems

## Scheduling and Notification of EO-1 Image Acquisitions

Note: This follows the path of information only, not image data.

traditional



Dash lines indicate future development of scheduling feedback so users know if their images have been scheduled.



# Solution



- If every node in a spacecraft or multi-spacecraft architecture writes status to an immutable block that is sync'ed every few minutes and is trusted, the only place users and systems have to go is the block
- Blockchain holds the history of all transactions
- Any new user only needs access to the block to get status and history
- Automatic easy extensibility for any system
- Previous example is just a single spacecraft, problem quickly becomes unmanageable with constellation

# Blockchain Components



Ledger		contains the current world state of the ledger and a Blockchain of transaction invocations
Smart Contract		encapsulates business network transactions in code. transaction invocations result in gets and sets of ledger state
Consensus Network		a collection of network data and processing peers forming a Blockchain network. Responsible for maintaining a consistently replicated ledger
Membership		manages identity and transaction certificates, as well as other aspects of permissioned access
Events		creates notifications of significant operations on the Blockchain (e.g. a new block), as well as notifications related to smart contracts. Does not include event distribution.
Systems Management		provides the ability to create, change and monitor Blockchain components
Wallet		securely manages a user's security credentials
Systems Integration		responsible for integrating Blockchain bi-directionally with external systems. Not part of Blockchain, but used with it.



# Public, Consortium, Private Blockchains Goddard SPACE FLIGHT CENTER

- **Public blockchains:** a public blockchain is a blockchain that anyone in the world can read, anyone in the world can send transactions to and expect to see them included if they are valid, and anyone in the world can participate in the **consensus process** – the process for determining what blocks get added to the chain and what the current state is. As a substitute for centralized or quasi-centralized trust, public blockchains are secured by **cryptoeconomics** – the combination of economic incentives and cryptographic verification using mechanisms such as proof of work or proof of stake, following a general principle that the degree to which someone can have an influence in the consensus process is proportional to the quantity of economic resources that they can bring to bear. These blockchains are generally considered to be “fully decentralized”.
- **Consortium blockchains:** a consortium blockchain is a blockchain where the consensus process is controlled by a pre-selected set of nodes; for example, one might imagine a consortium of 15 financial institutions, each of which operates a node and of which 10 must sign every block in order for the block to be valid. The right to read the blockchain may be public, or restricted to the participants, and there are also hybrid routes such as the root hashes of the blocks being public together with an API that allows members of the public to make a limited number of queries and get back cryptographic proofs of some parts of the blockchain state. These blockchains may be considered “partially decentralized”.
- **Fully private blockchains:** a fully private blockchain is a blockchain where write permissions are kept centralized to one organization. Read permissions may be public or restricted to an arbitrary extent. Likely applications include database management, auditing, etc internal to a single company, and so public readability may not be necessary in many cases at all, though in other cases public auditability is desired.

Source: <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>