### Cybersecure Modular Open Architecture Software Systems for Stimulating Innovation

Walt Scacchi and Thomas Alspaugh



**INSTITUTE** for **SOFTWARE RESEARCH** UNIVERSITY of CALIFORNIA · IRVINE

## Overview

- Background: Problem and Solution
- Blockchains and Smart Contracts
- Software Supply Chains and Ecosystems
- Software Development and Evolution Update Transactions
- Case Study: Evolving installed software configurations of Open Architecture command and control/business systems
- Conclusions

## Background

- Problem: How best to develop and demonstrate new conceptual approach to providing continuous cybersecurity assurance with OA C2 software systems subject to frequent evolutionary updates?
  - This is our *stimulus* for innovation

## Background

- <u>Solution</u>: Utilize tools and techniques for Blockchains and Smart Contracts to continuously assure the cybersecurity of OA software systems as they undergo software development and evolutionary updates.
  - Why? to assure the integrity of updates to individual systems distributed across open networks, and to prevent cyber attacks to software supply chains and ecosystems.
  - This requires software development and evolution process *innovation*!

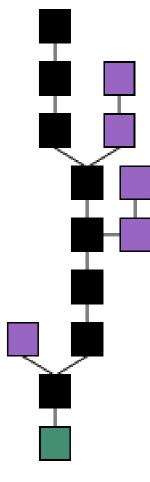
### Blockchains

Blockchains represent *append-only*, decentralized "bookkeeping" *ledgers* of incoming/outgoing *enterprise transaction blocks* in a denominated currency or resource (e.g., BitCoin, Gold, Artworks).

•Decentralized counterpart to "centralized ledgers with central authority" (e.g., bank accounts).

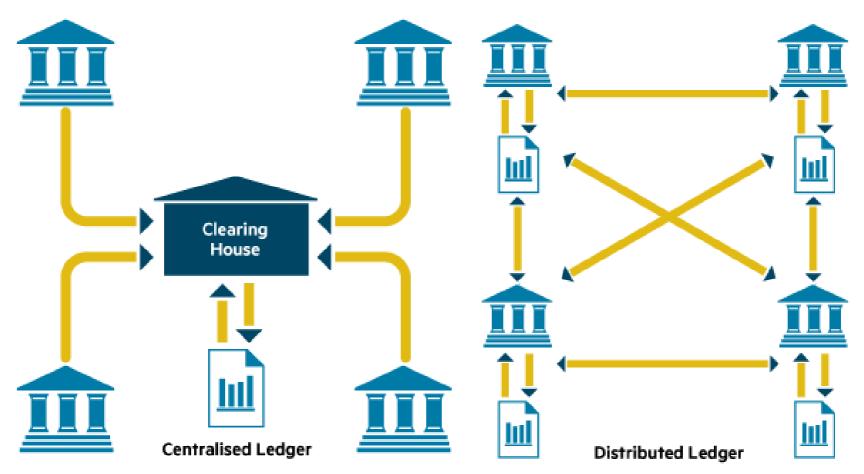
 Accommodate anonymized transactions and transaction verifications without central authority.

•Updates to blockchain can require update providers to pay a fee for an update transaction verification.



#### Embedding distributed ledger technology

A distributed ledger is a network that records ownership through a shared registry



In contrast to today's networks, distributed ledgers eliminate the need for central authorities to certify ownership and clear transactions. They can be open, verifying anonymous actors in the network, or they can be closed and require actors in the network to be already identified. The best known existing use for the distributed ledger is the cryptocurrency Bitcoin

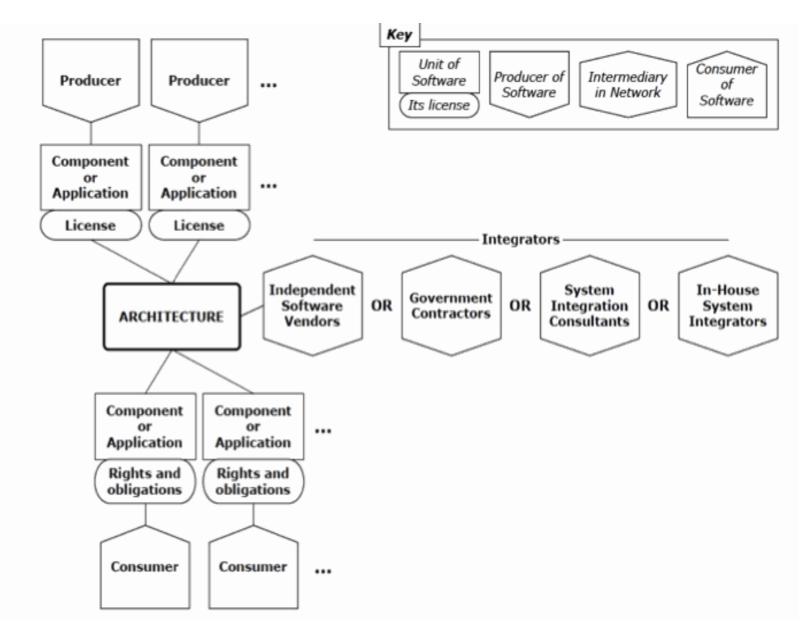
FT graphic. Source: Santander InnoVentures, Oliver Wyman & Anthemis Partners

## **Smart Contracts**

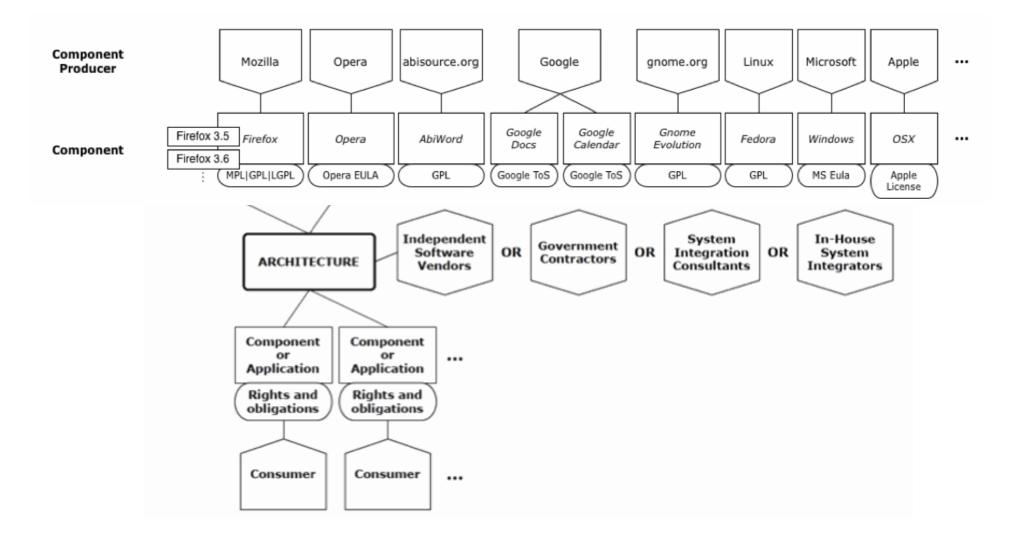
Contracts that specify a block of transactions (including obligations and rights) between parties that can be formally expressed using computational (source) code.

- Computational contracts can be *interpreted and enforced automatically* via computer-based
   transaction processing systems.
- Accommodates establishment of complex *multi-party trading/sharing agreements* between known, unknown, or untrusted parties.

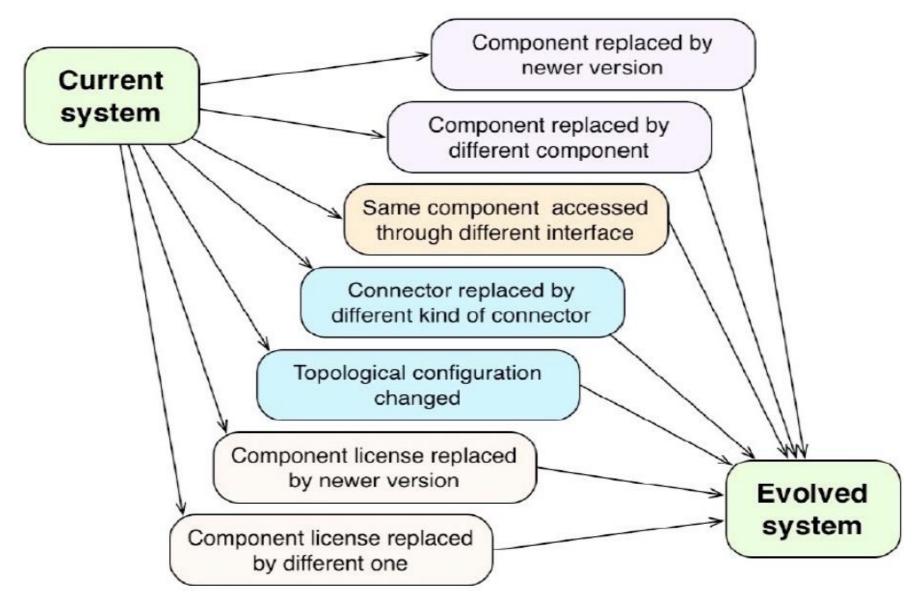
# Software supply chains across an OA software system ecosystem



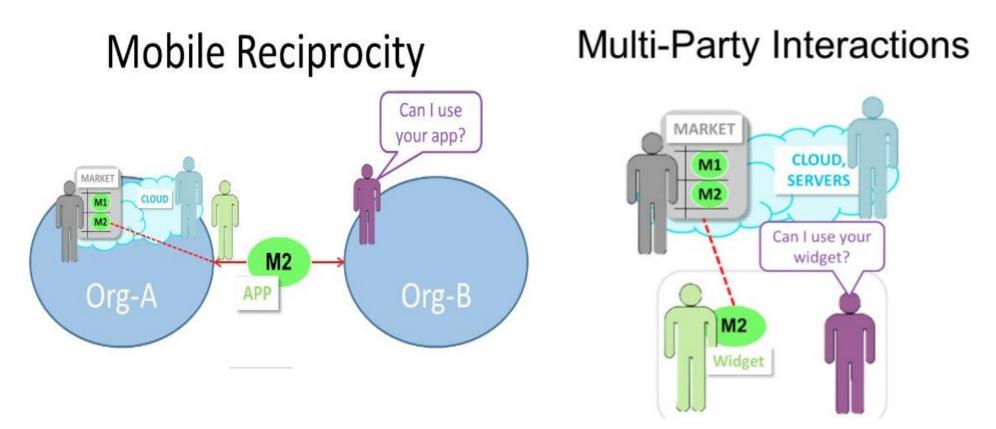
#### Software supply chains across *multiple component producers* in an OA software system ecosystem



### Types of software evolution updates

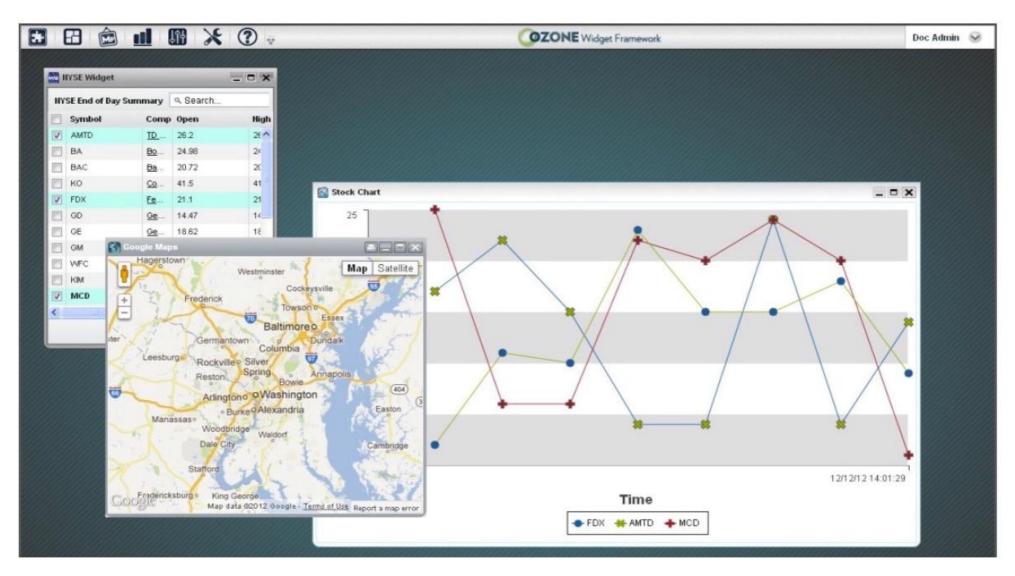


Case Study: Evolving installed software configurations of Open Architecture command and control/business (C2/B) systems C2/B enterprises moving to multi-party acquisition of OA software elements within ecosystems (Scacchi and Alspaugh 2015, 2016)



Customer/end-user organizations now looking for ways to reduce acquisition cost and effort through *shared development/use of common OA software system components* (apps, widgets).

# OA system development using inter-communicating widgets/apps acquired from online App Stores



Installed software configuration using Ozone apps and widgets as OA system components for desktop/mobile laptop computers



# Deployment scenario for Apps and Widgets as OA system components



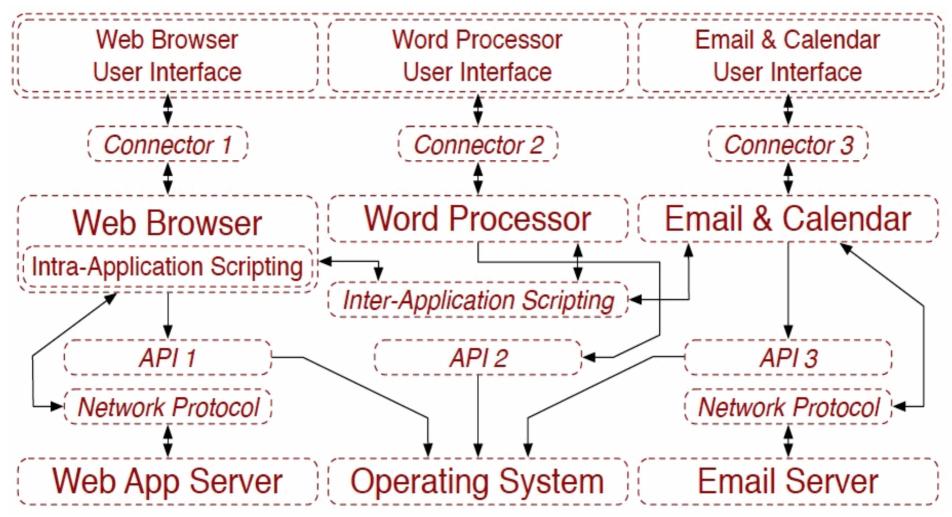
Installed software configuration for mobile devices

# Deployment scenario for Apps and Widgets as OA system components

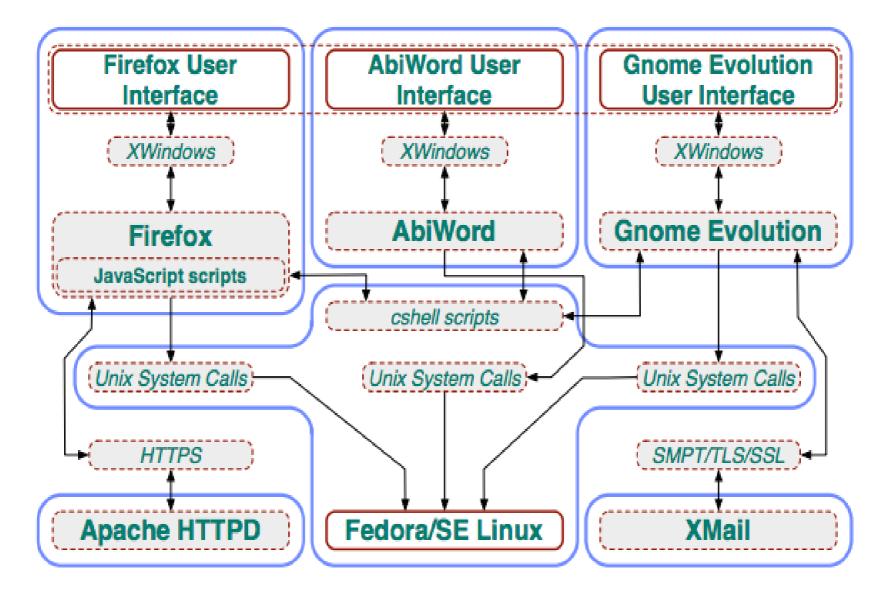


#### Installed software configuration for *Future Command Center*

# Design-time view of an OA system configuration



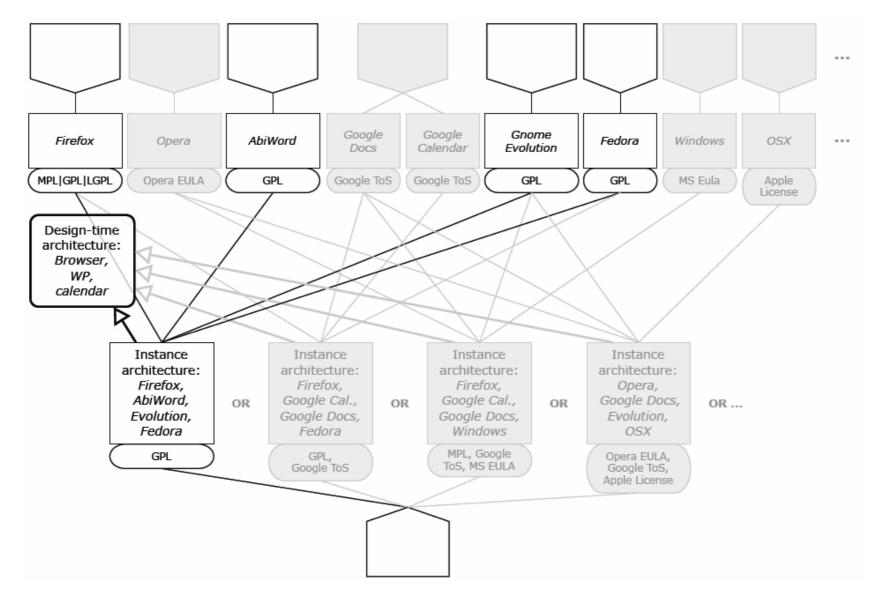
# *Build-time* view of OA system configuration incorporating component security encapsulations



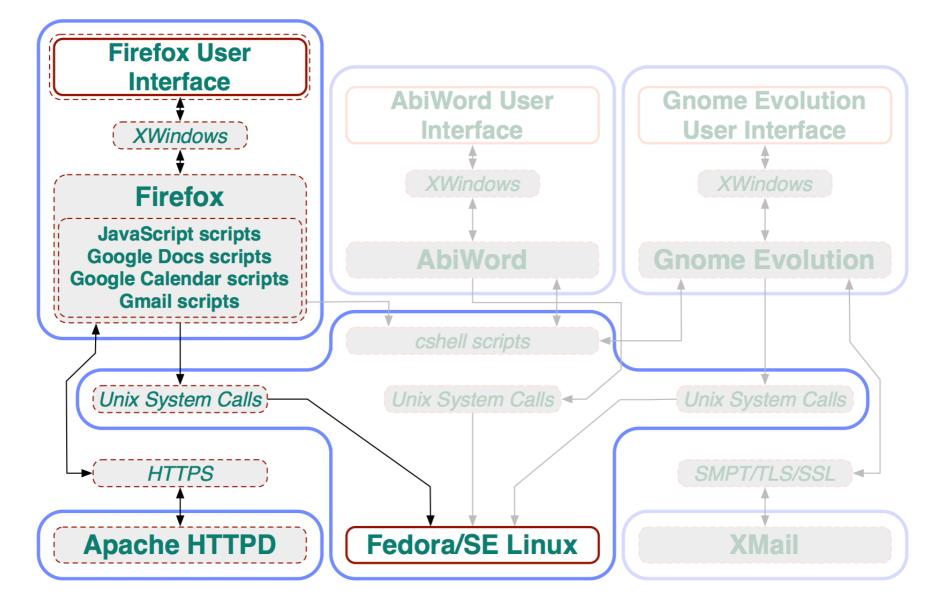
# Run-time deployment view of OA *installed software configuration*

Die Est View Higtory Bookmarks (Sink 1946) the Sin Control of Single Si	Clie Lit Yew Artions Search Help	
	New Send / Receive Print Previous Today Next	Go To Day
GAME CULTURE & TECHNOLOGY LAB		Search 🗃 Summary Contains 🖉
GAME COLITIKE & TECHNOLOGY LAB	Winday 12 january	Tasks
	v On This Computer	Chck to add a task
💓 🔍 🔍 🖤 🐨 📥 💖 🔢	9 am	L : 1
X = / =	10 arthdays & Arrivers.	
0404582 EP		Hemes
English Exercision	11 am	Click to add a memo
Search C. Palanced Search	film the vice that de fait fait	
a provide a second s	2 / = :: 1 2 3 4 1pm	il i 🥼
Package	5 6 7 8 9 10 11 2 pm	- E 🖊
Comming Signal or indicated version at the OCTL period subman. This appen sequence distribution of the new time get to these of you who may want to so the get colladoration indicating of the low. That signal between it and the VER MILLION	13 13 14 15 16 17 18	
attactive a part of the second s	19 20 21 22 23 34 25 3 <sup>pm</sup>	THE .
Face-United Biol Science Vol 10	26 27 28 29 30 31 4 Pm	Gnome Evolution
Firefox Production Child Child Child Child	5 P P P P P P P P P P P P P P P P P P P	
evening prove lidentifiers)	6 <sup>pm</sup>	email, calendar
News Finishe gamp Comparison     Document Version Control System (saling DRM v115)     Document Version Control System (saling DRM v115)		· · · · · · · · · · · · · · · · · · ·
Search Engine and Constor ( Joint Down)		
Ble Edit View Insert Format Jools Table Collaborate Documents Help	Tasks Memos 8 Pm	a :/
😑 🚨 🙆 🚖 🍐 👙 🖉 👘 🏙 Page Width 🗸		
Normal v Times New Roman v 12 v a a a	F - B Edt Vew Jerninal Jahn Belp	
	ipitables-multi poncia-secket-startup upremies	Red Hat /
biWord Notes on Open Source Software and Open Architectures	Applicables save player, rest ups Applicables save player, rest ups	
The second provide New Associate, and New Rowshill With a second provide New York Street Stre	spisies plysouthd upplit     spisies with portrelease weak-modules	Fedora Linux
	Eistables-restore portreserve splint E[liveuser@localhost /]5 is	
	Boar dey have lost-found ant proc shin sry an war boar atc lin wedla out root sellmus ups ear	
	#[llvmiser@localhost /]\$ is /selinum access compatinet initial contexts policyvers	
A CONTRACTOR OF A CONTRACTOR O	alarc context load reject unknown boolwant create member relatel	
a company of the second s	checkreeprot deny unknown mis user	

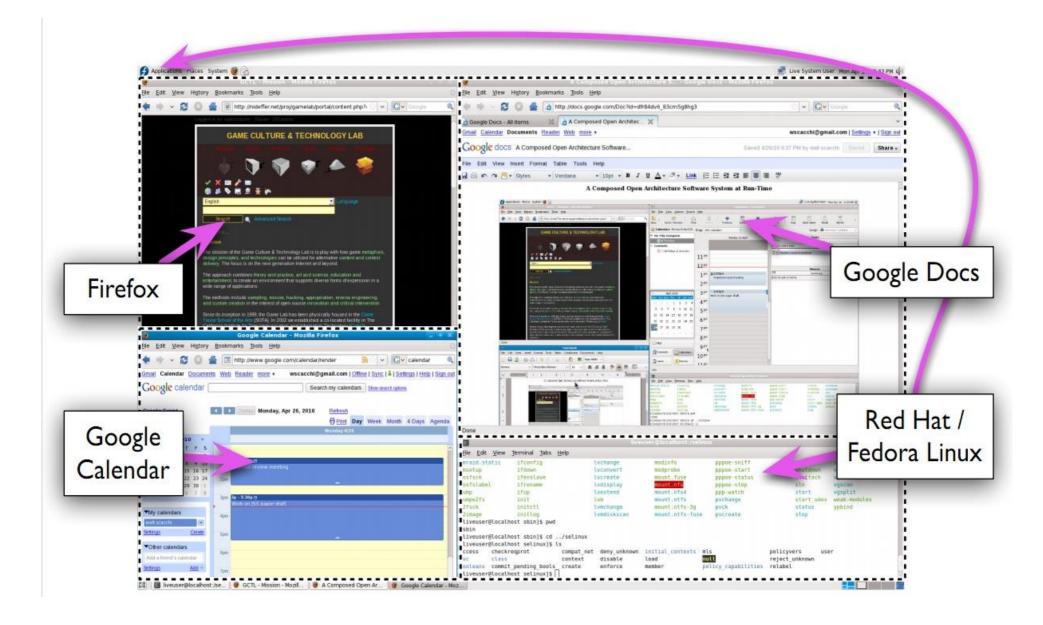
# Software supply chain giving rise to the installed software configuration



# Build-time view of OA installed software configuration *after* evolutionary update transactions



# New run-time deployment view of installed software configuration following multiple evolutionary updates



### Observations

- Blockchains and smart contracts can be utilized to specify and implement evolutionary updates to installed software configurations of OA C2/B systems
  - assure the integrity of ISC updates to individual systems distributed across open networks.
    - smart contracts can be used to automate ISC update
       processes
    - transaction verifiers can manage/track anonymous parties providing updates, and charge fees for verification!
  - prevent cyber attacks to Defense/commercial software supply chains and ecosystems that produce and integrate software component updates.
    - blockchains can be used to identify compromised ISC before/after planned evolutionary updates!

## Conclusions

Software supply chains are the primary channel through which large scale cyber attacks are transmitted.

- Blockchains and smart contracts are a promising new approach to assuring the cybersecurity of OA software systems, and the software supply chains that provide ongoing streams of evolutionary updates to installed software configurations.
- Blockchains and smart contracts are also applicable to other acquisition activities
- Blockchains and smart contracts merit further research and development for use in acquisition of OA software systems for command and control/business enterprises.

## Acknowledgements

Research collaborators

Cybersecurity Policy & Research Institute (CPRI) at UCI

Funding support (No endorsement, review, or approval implied).

Naval Postgraduate School

Acquisition Research Program Grant

#N00244-1-16-0053.

# Thank you!

