WORKSHOP AREAS of FOCUS

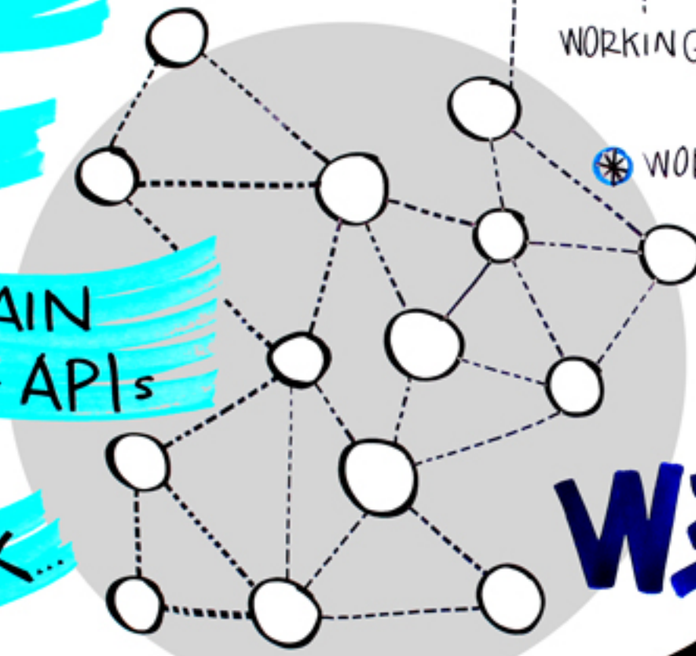
IDENTITY

PROVENANCE

BLOCKCHAIN PRIMITIVES & APIs

the KITCHEN SINK....

BLOCKCHAINS & the WEB



W3C

W3C VOLUNTARY STANDARDS SETTING STEWARDING the OPEN WEB

PUBLICATION of STANDARDS

RECOMMENDATION TRACK

WORKING GROUPS

WORKSHOPS and COMMUNITY GROUPS

WHAT DOES the WEB NEED to SUPPORT & INTERFACE BETTER?

and

HOW CAN the TECH of BLOCKCHAIN SUPPORT the WEB?

CLIENT SIDE FEATURES

DATA and FORMATS

COMMUNICATION PROTOCOLS

RELEVANT WORK

- SECURITY & PRIVACY
- WEB AUTHENTICATION
- WEBCRYPTO API
- WEB APP SECURITY
- ENCRYPTION EVERYWHERE
- WEBPAYMENTS

DOUG SCHEPERS and WENDY SELTZER

#BLOCKCHAINWEB

IRC.W3.ORG (#BLOCKCHAIN)

W3C | Blockchains & the Web Workshop

June 29-30, 2016 | MIT Media Lab

dpict.

the SECRET SAUCE of COLLABORATION

- DELIBERATING v. CONSENSUS
- FRAME and SET UP the CONVERSATION UP FRONT
- LISTENING & OPEN COMMUNICATION
- TALKING ≠ COMMUNICATION
- TRUST
- WORK to ACHIEVE COLLABORATIVE CONSENSUS
  - STOP, SUMMARIZE/ WRITE DOWN to ENSURE COMMON LANGUAGE and UNDERSTANDING
- HEALTHY FRICTION
- COMPETITION and COLLABORATION (Hand in hand)
- SIDESTEP PROPRIETARY INTEREST and STALE THINKING!
- SHARED PROBLEM STATEMENT a COMMON GOAL!
- KNOW WHEN YOU'RE FINISHED/ WHEN to STOP
- FLEXIBILITY & DIVERSITY
- CONNECT to IMPACT
- MOTIVATION ABOVE & BEYOND
- FAIL FAST and STAY FOCUSED
- ENCOURAGE EARLY ADOPTERS THROUGH HANDS-ON PLAY
- OWNERSHIP of the ISSUE – CLOSEST to the CLIENT
- DEFAULT TOWARDS OPEN!

W3C | Blockchains & the Web Workshop
June 29-30, 2016 | MIT Media Lab

dpict.

PUBLIC v. PRIVATE

- APPEND-ONLY LOG USING HASH POINTERS/ MERKLE TREES
- CRYPTOGRAPHIC ID
- PROOF of WORK
- NAKAMOTO CONSENSUS
- CURRENCY
- + BYZANTINE CONSENSUS

(CAN'T GENERALIZE ABOUT ALL BLOCKCHAINS)

BITCOIN
- NO MAJOR FUNDAMENTAL PROBLEMS (CAVEAT: END POINT SECURITY)

HUMAN-CRYPTO INTERACTION is an UNSOLVED PROBLEM!

STANDARDIZATION MAY HELP HERE
- AN OPPORTUNITY for INTROSPECTION
- ENABLES REGULATION
- ENABLES 'LEGIBILITY'

the POWER of BLOCKCHAINS

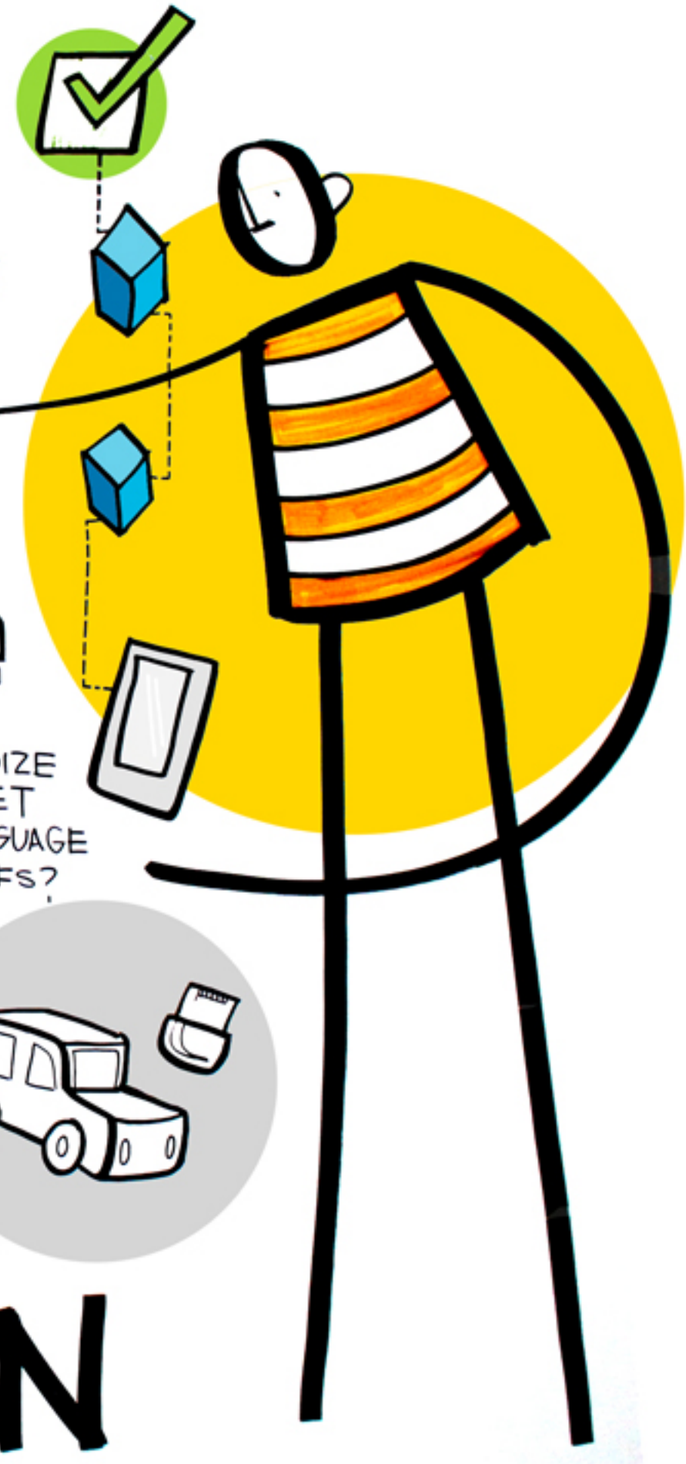
the REACH of the WEB

ENABLING NEW APPLICATIONS

BLOCKCHAINS, the WEB & STANDARDIZATION

PROOFS
- STANDARDIZE a SMALL SET OR a LANGUAGE for PROOFS?

VERIFIERS COULD BE OFFLINE (CLIENTS CAN BE THIN and DUMB)

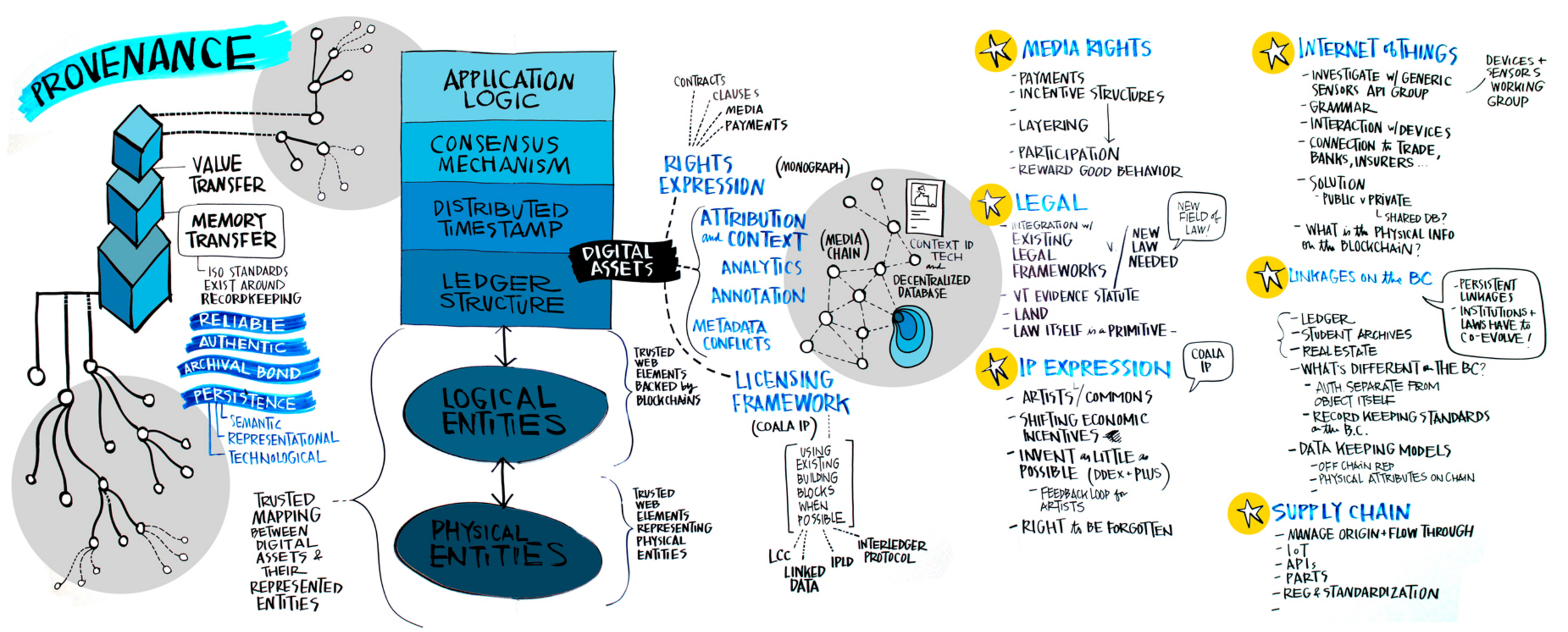


ARVIND NARAYANAN

W3C | Blockchains & the Web Workshop

June 29-30, 2016 | MIT Media Lab

dpict.



W3C | Blockchains & the Web Workshop

June 29-30, 2016 | MIT Media Lab

dpict.

IDENTITY

- OPEN SYSTEM
- USER-SOVEREIGN IDENTITY
- MEMORABLE IDENTIFIERS
- INDEXABLE REGISTRY
- SEMANTIC DATA

PEOPLE · ORGS · DEVICES · IDEAS

TRUE ENTITY PERSISTENCE → (BUNDLES OF ATTRIBUTES)

see SHIP of THESEUS

- USER SOVEREIGN
- DECENTRALIZED
- DISTRIBUTED
- PROOF OF OWNERSHIP

PROBLEMS OF:

DATA PRIVACY

TRUST (TECHNICAL v. SOCIAL)

ID ANCHORED + ENABLED BY the BLOCKCHAIN

- NEVER ALLOW RAW DATA to LEAVE REPOSITORY!
- DATA ENCRYPTED at ALL TIMES!
- ALWAYS RETURN AGGREGATE ANSWERS!

- QUALITY
- SECURITY
- FREEDOM / INDEPENDENCE
- SOURCE
- PRIVACY
- BINDING to REAL WORLD
- ATTRIBUTES
- PROVENANCE / TRUST
- AVAILABILITY / PERSISTENCE
- AUDITABILITY

IDENTITY for EVERYONE

- BIOMETRIC ATTESTATION
- #, SIZE, CONNECTIONS
- UTILIZATION
  - PAYMENTS
  - MUTUAL ASSETS
  - SERVICES

OVERALL ARCHITECTURE of BC IDENTITY SYSTEMS

- WHAT BELONGS / DOESN'T
- WHERE + HOW STORED
- REDUNDANCY
- ZONE FILES and POINTERS
- HARDWARE
- STORAGE & KEYS
- MULTIPLE IDs
- PRIVACY + DATA LIMITATION
- AS LITTLE AS POSSIBLE SHOULD BE STORED in B.C. (COMMON, MINIMAL CORE)

ARCHITECTURE STANDARD · ROLES · DNS ZONE FILES

TRULY UNIVERSAL
an OPEN STANDARD on an OPEN PLATFORM

MANY OPPORTUNITIES!

VERIFIABLE CLAIMS DATA MODELS

JOIN the V.C. TASK FORCE!

- PRIVACY
  - SELECTIVE DISCLOSURE
  - EDITING / STORAGE
- WORK w/ CURRENT LEGAL FRAMEWORK
- BC NOT a PANACEA
- ECONOMIC INCENTIVES
- LIFETIME - RIGHT to BE FORGOTTEN?

EFFICIENT THIN CLIENT VERIFICATION of IDENTITY

- NON MEMBERSHIP PROOF PROBLEM
- FRESHNESS PROBLEM
  - INDEX DATA + COMMIT
  - LINEAR COMMITMENT
- ☐ PROOF of WORK
  - QUERY for HASH CHAINS
- ☐ CLASSICAL BFT SYSTEM
- ☐ ORACLE SYSTEM
- ☐ OUT of BAND COMMUNICATION

TOO MUCH IDENTITY!

- LEAST POSSIBLE!
- SPECTRUM

NOTHING · EPHEMERAL · PERSISTENT · LINKED PERSISTENT to BIOLOGICAL ID / LEGAL ID (ONLY if NEEDED)

- USE ATTRIBUTION OR EPHEMERAL ID WHEN POSSIBLE

HYPERLEDGER, IBM MEMBERSHIP SVCS ARCHITECTURE

- CENTRALIZED + DECENTRALIZED SVCS
- LT + SHORT TERM ID PIECES
- PRIVATE + PERMISSIONS LEDGERS
  - LONG LIVED / AUTHORIZATION CERTS
  - TRANSACTIONAL CERTS
    - REDUCE / PREVENT CORROLATION
  - SPECIFICITY MAY GO DOWN OVER TIME
  - RELY ON 3RD PARTY VENDORS

BC STANDARDS in HEALTHCARE

- CONNECTION to EXISTING LEGAL STRUCTURES / REG. REQMT'S
- DRIVE COST of OWNERSHIP to EDGES
- AGGREGATION ISSUE & TRANSACTIONAL ISSUE
- SAFEGUARD INTEGRITY
- LEAVE DATA at POINT of ORIGIN

STANDARDS
- ☐ BC + SELF SOVEREIGN ID
- ☐ AUTHORIZATION
- ☐ DIGITAL POST-MARK

TECH
- SELF SOVEREIGN MOBILE
- SELF SOVEREIGN SERVER
- REPUTATION

W3C | Blockchains & the Web Workshop
June 29-30, 2016 | MIT Media Lab

dpict.

W3C | Blockchains & the Web Workshop

June 29-30, 2016 | MIT Media Lab

dpict.

W3C COMMUNITY (DISCUSSIONS)

DIGITAL ASSETS
☆ @KS91020, TARIQUE BHUIYAN
- IDENTIFY PROBLEMS
- IDENTIFY SUB GROUPS
- IDENTIFY USE CASES
  - START DEFINING COMMON ATTRIBUTES BASED ON USECASES

KEY MGMT OUTSIDE the BROWSER
☆ WON-BEON KIM
- IDENTIFY EXISTING STANDARDS
- DISCUSS USE CASES

SMART SIGNATURES
☆ ADRIAN HOPE-BAILIE, EVAN SCHWARTZ, CHRISTOPHER ALLEN, PETER TODD, RYAN SHEA
- PUBLISHING FINAL DRAFT of WHITE PAPER in 2 WEEKS
- DEX INITIAL SPEC

BEST PRACTICES RE: SECURITY
☆ JOSH, GERRY, GLADIS F.
- TRACK OTHER COMMUNITIES & STANDARDS BODY & UNDERSTAND HOW IT CONTRIBUTES to SECURITY STANDARDS
- DEFINE SECURITY & RISK REQUIREMENTS/PROFILES
- GLOBALLY DISTRIBUTED TESTNETS for ATTACKS & TESTS

DEMO
☆ RICK DUDLEY, ADRIAN GROPPER
- WEBAUTH
- VERIFIED CLAIMS
- BLOCKCHAIN ID
- BLOCKCHAIN RECEIPTS
- OAUTH2/UMA AUTH

INTER-LEDGER
☆ ADRIAN HOPE-BAILIE, EVAN SCHWARTZ

BLOCKCHAIN VOCABULARIES - BLOCK CHAIN VOLTRON
☆ RICK DUDLEY
- BEGIN DISCUSSIONS/IDENTIFYING COMMUNITY (CONTACT ALAN + MANU)
- DRAFT VOCAB?
- INITIAL SCOPING - ID SUBVOCABS

STANDARDIZE INTERFACE of CONSENSUS LOGIC
☆ ETHAN BUCHMAN

W3C STANDARDS (SPECIFICATIONS)

BLOCKCHAIN ID AUTH
☆ DANIEL BUCHNER, RYAN SHEA
- BEGIN DISCUSSIONS w/ EDGE & SAMSUNG BROWSER TEAMS ABOUT an EXPERIMENTAL PROTOTYPE
- INVESTIGATE REQUIRED SPEC ADDITIONS to LEVERAGE BLOCKCHAIN IDENTITIES VIA WEB AUTH

IPLD & MULTIFORMATS
☆
- CALL for PEOPLE to FORM WORKING GROUP (W3C or IETF)
- DECIDE HOME for EACH PROTOCOL (W3C OR IETF)
- WRITE SPEC DRAFTS 2 SUB (DRAFT READY)
- COMMIT to WORK TASKS & PIPELINE SO COMMUNITY CAN CONTRIBUTE
- PUBLISH "IPLD PLAYGROUND" (IPLD.IO)
- PUBLISH "MULTIFORMATS PLAYGROUND" (MULTIFORMAT.IO)

PROOF & VERIFICATION
☆ RICK DUDLEY, WAYNE VAUGHN, ETHAN & JAE
- PUBLISH CHAINPOINT 2.0
- FORMALIZE TENDERMINT SPV
  → GENERALIZE for OTHERS (MAYBE USING IPLD, DEX, ETC)

LIBP2P
☆
- GATHER INTERESTED PEOPLE in THIS (+OTHER) GROUPS
- FINISH WRITING CURRENT REVISION of PROTOCOL INTERFACES
- CREATE a SUB-PROTOCOL COMPLETENESS PIPELINE (SPECS, IMPLS, CROSS IMPL TESTS, PLAYGROUND)
- PUBLISH LIBP2P.IO FOR AWARENESS and DOCS
- FIGURE OUT WORKING GROUP HOME + TRAJECTORY (INVOLVE IETF?)

W3C | Blockchains & the Web Workshop
June 29-30, 2016 | MIT Media Lab

dpict.