Blockchain and Distributed Ledger Technologies:

Opportunities, Challenges and Future Work

Andrew Regenscheid

Cryptographic Technology Group

NIST

National Institute of Standards and Technology

Technology Administration, U.S. Department of Commerce

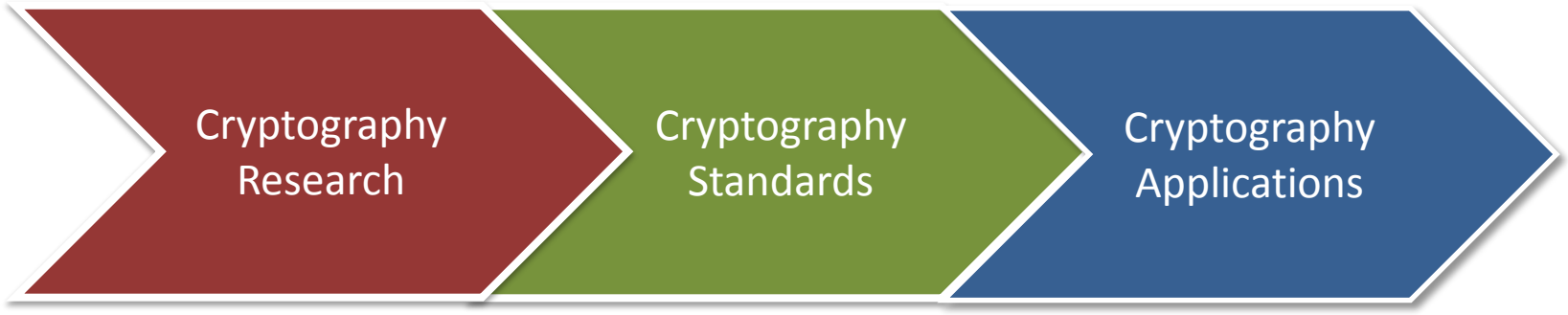
Cryptographic Technology Group

Mission:

Research, develop, engineer, and standardize cryptographic algorithms, methods, and protocols.

Goal:

Promote the adoption of strong cryptography through fundamental research, and the development of standards, guidelines, tools and metrics.



National Institute of Standards and Technology
U.S. Department of Commerce

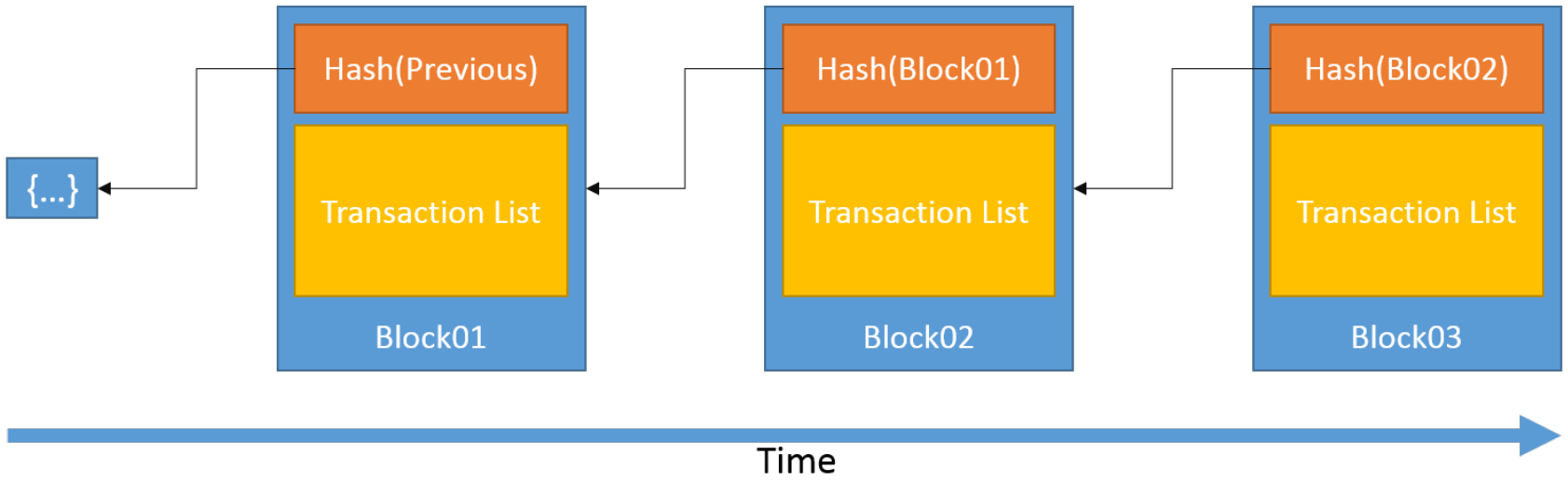
Blockchain is…

A **distributed ledger** which is:

- *Decentralized*
- *Peer-to-peer*
- *Tamper-evident/resistant*
- *Synchronized through consensus*

Facilitate transactions between mutually-distrusting entities without the need for a trusted arbiter

Hash Chain



Permissionless Blockchains

Characteristics:

- Participation open to the **public**
- **Peer-to-peer** transactions
- Typically tied to **cryptocurrency**
- Fully **decentralized**

Challenges:

- **Privacy** and **scaling**

Permissionless blockchains are a disruptive technology that can dramatically change how we conduct business activities.

Permissioned Blockchains

Characteristics:

- Participation can be **private** and/or **controlled**
- **Trusted** participants
- More **efficient** than many public blockchains
- Can support **privacy** and **confidentiality** in transaction

Challenges:

- Some level of **centralized trust** through governing authority

Permissioned blockchains may lead to cost-savings, workflow improvements, automation and improved auditing with current business processes.

Use Cases

- Financial Services
- Data/Asset Registries
- Provenance/Supply Chain
- Identity management
- Voting
- ….

The list goes on and on…

Areas for Further Research

- Security
- Privacy
- Scalability
- Consensus Algorithms
- Quantum-Resistance

Standards

- Active Standardization Efforts
  - International Standards: ISO, IEEE
  - National Standards: ANS X9
  - Industry Consortia: Hyperledger, W3C
- Current and future work items
  - Terminology and taxonomy
  - Use cases
  - Blockchain interoperability
  - Primitives and building blocks

Cryptographic Primitives

- Foundations in existing cryptographic standards
  - Hash functions
  - Digital signature algorithms
- Potential for future work on:
  - Ring signatures
  - Threshold signatures
  - Bit commitment schemes
  - Zero knowledge proof techniques
  - Multiparty Computation
  - Quantum-resistant algorithms

Operational Considerations

- Deployment and operational security best practices for nodes and private blockchains
- Identity and Access Management- Particularly for Permissioned Blockchains
- Security of wallets and user/transactional identities and credentials
- Mitigating risks associated with irreversible transactions

NIST Activities

- Established internal testbed to explore blockchain technologies and use cases
- Participation in standards activities
- Investigating blockchain use cases
  - Co-hosted "*Blockchain and Healthcare Workshop*" with HHS in 2016
- Foundational research in blockchain architectures, taxonomies, and cryptographic primitives

Questions?

Contact Information

Andrew Regenscheid

Andrew.Regenscheid@nist.gov

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Blockchain Workbench

dylan.yaga@nist.gov
NIST/ITL/CSD
Security Components and Mechanisms Group
6.28.2017

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

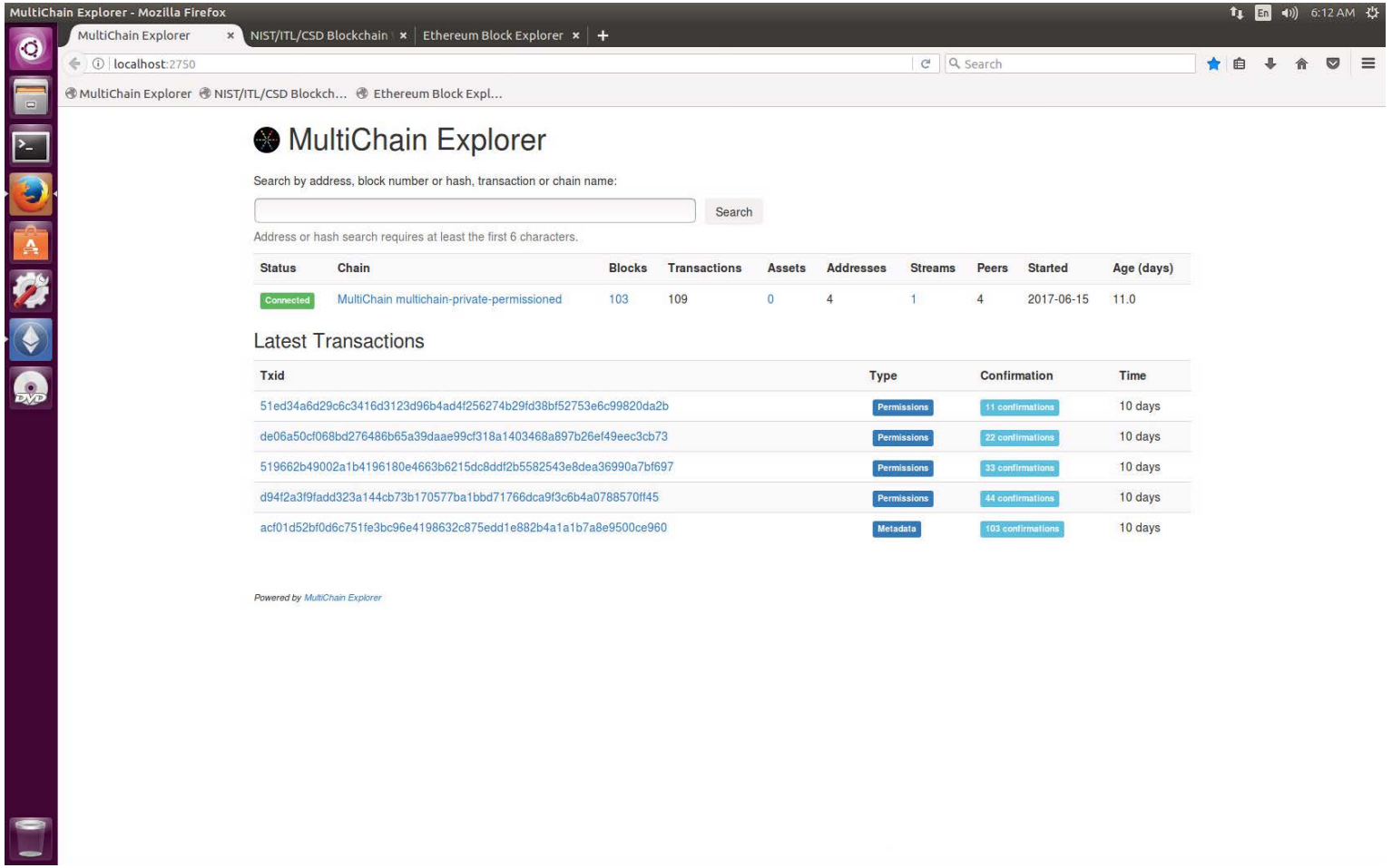
NIST Internal Workbench Rationale

- Great deal of interest in blockchain within NIST
  - Not a lot of expertise or experience – yet!
- Uncertainties understanding how to proceed with real world blockchains and dealing with the purchase of cryptocurrencies for experimentation
- Would be inefficient for every researcher with interest to:
  - Determine which blockchain to choose
  - Learn methods for initializing a blockchain node
  - Construct and operate a distributed blockchain network

Initial Workbench Implementation

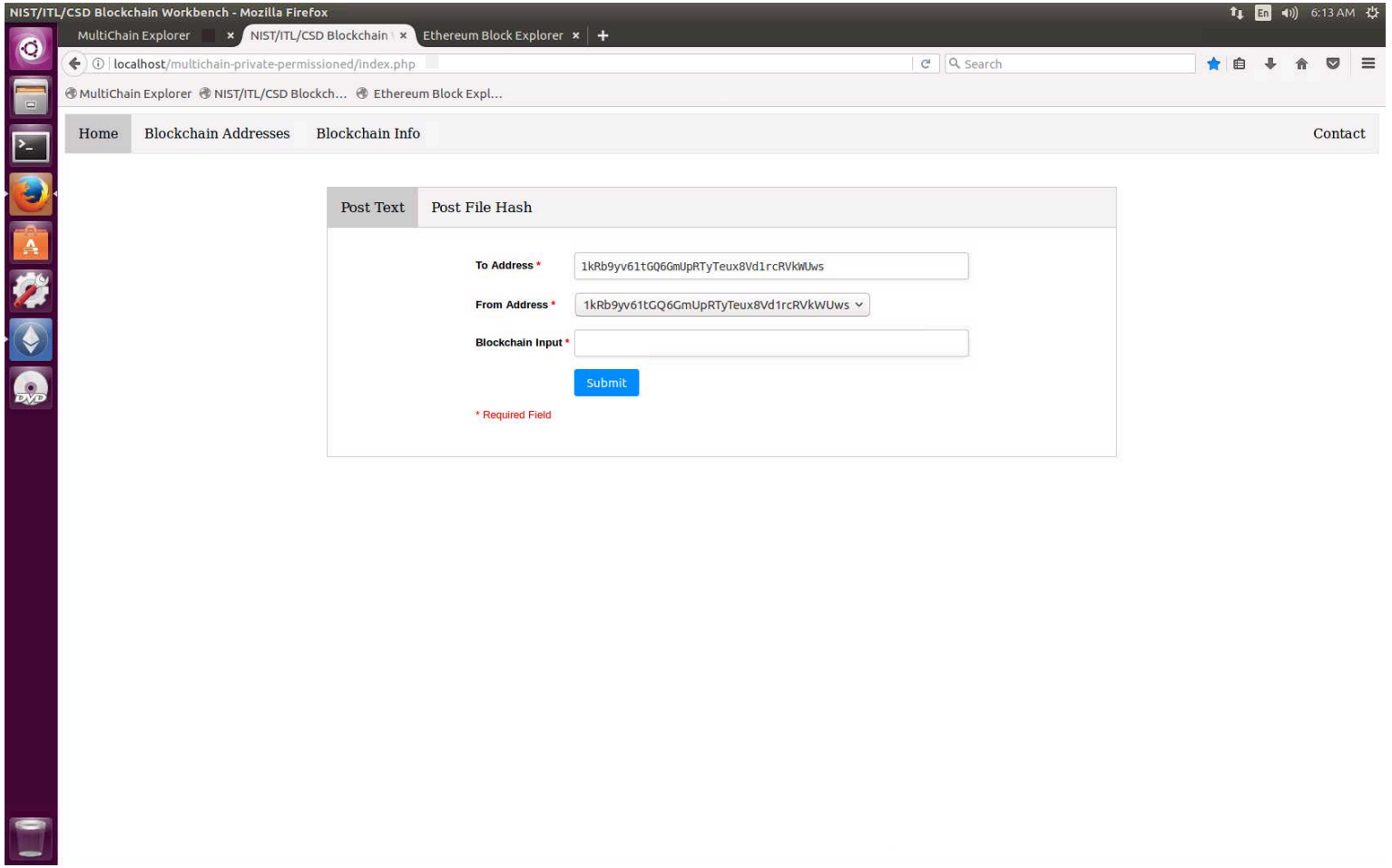
- Still under development; starting small – but can easily be scaled
- 5 node virtual machine cluster running instances of Ubuntu 16.04 Server
- Working with widely used Open Source Software when possible – in order to ensure experiments can be translated to real world environments
- Initial blockchain offerings
  - MultiChain – running in private and permissioned mode; not Proof of Work
  - Ethereum – allowing for the experimentation with Smart Contracts
  - Hyperledger – a feature rich blockchain, with a lot of industry interest
- Demonstration applications

Workbench – MultiChain Explorer



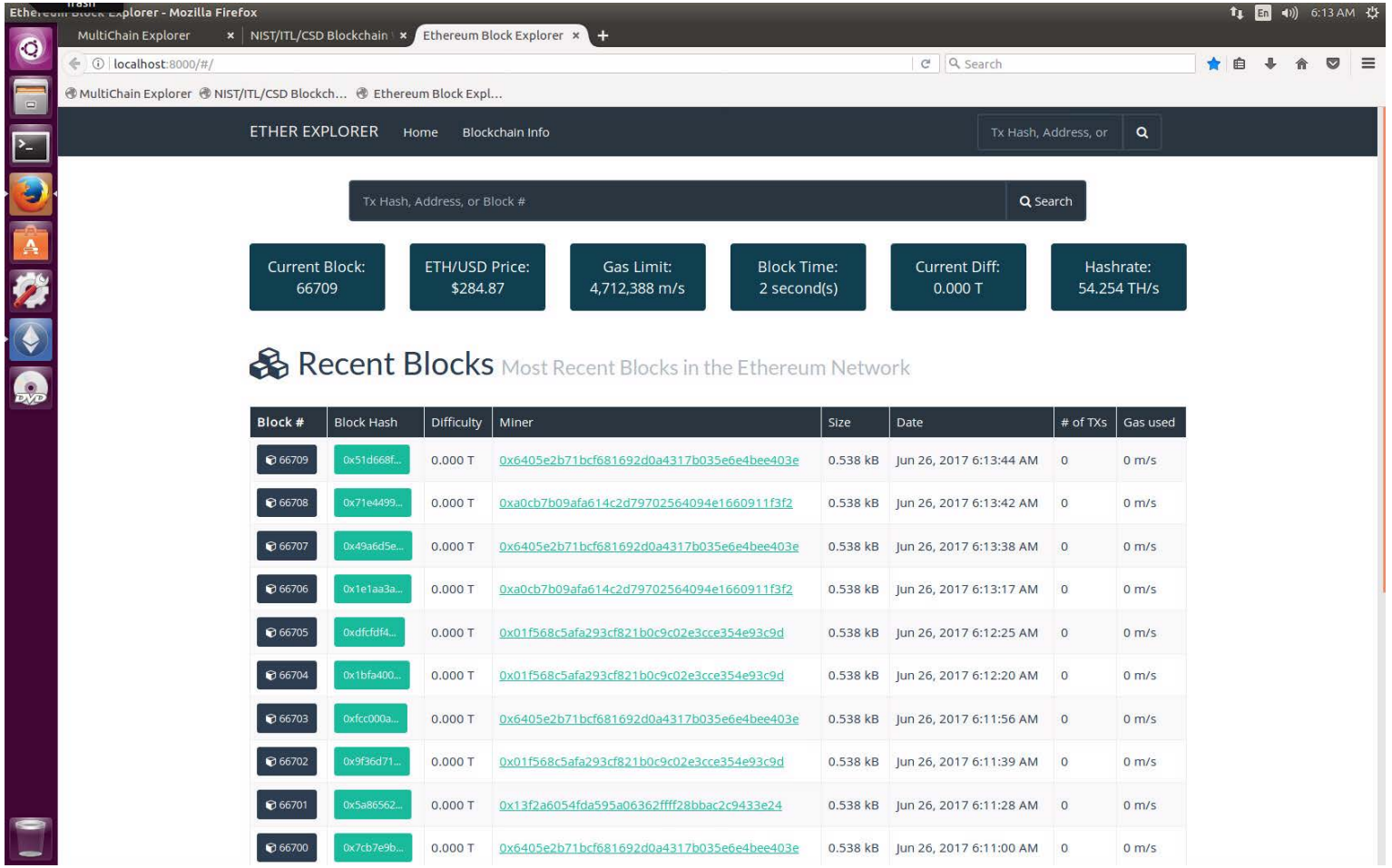
National Institute of Standards and Technology
U.S. Department of Commerce

Workbench – Demo Application



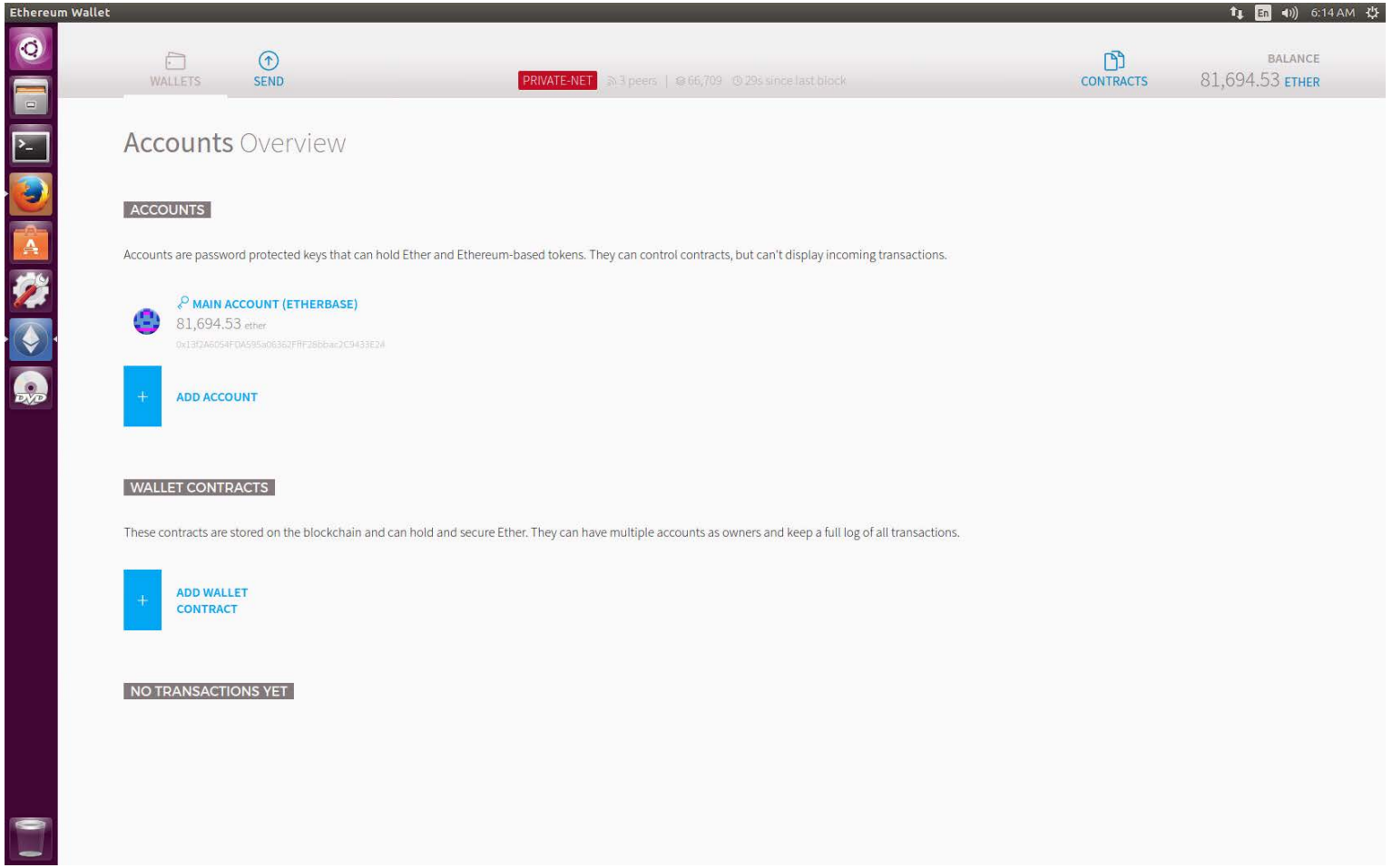
National Institute of Standards and Technology
U.S. Department of Commerce

Workbench – Ethereum Explorer



National Institute of Standards and Technology
U.S. Department of Commerce

Workbench – Ethereum Mist Wallet



Workbench Deliverables

- The actual Workbench itself
- Initialization & setup scripts
- Demonstration application source code
- User documentation
- Any development insights documented

```
#!/bin/bash
################################################################################
#Script: setup_multichain_private_permissioned.sh
#Purpose: To Download, Setup & Configure, Launch MultiChain Blockchain Platform,
#         Blockchain Explorer, and associated Web Demos for the NIST/ITL/CSD
#         Internal Blockchain Workbench
#Tested On: Ubuntu 16.04 Server & Desktop
#Author: Dylan Yaga
#Email: dylan.yaga@nist.gov
#
#
################################################################################

################################################################################
#Variables
################################################################################
#Variables that can be changed to alter the names of the blockchain
blockchain_name=multichain-private-permissioned
web_folder=/var/www/html/$blockchain_name
explorer_name=$blockchain_name-explorer
blockchain_folder=/home/$USER/$blockchain_name
explorer_folder=$blockchain_folder/multichain-explorer/multichain-explorer-maste
#Boolean to determine whethere or not to use the embedded base64 webpage
#resources
use_embeded=true
################################################################################
```


National Institute of Standards and Technology
U.S. Department of Commerce

Why no Bitcoin Blockchain?

- Just an initial choice
- MultiChain is API compatible with Bitcoin, so applications written for it are easily transferrable to Bitcoin
- No need to expend CPU and power on Proof of Work
- Can easily set it up as an additional blockchain later

Initial Demonstration Applications

- Hashed Text Posting
  - Website accepting arbitrary text, hashing it with SHA256 and allowing an optional 8-character TAG to be prepended to it
  - Reason – shows simple use of APIs for developers to learn from initially
- Document Proof-of-Existence
  - Users can upload files, have it hashed with SHA256 and the resulting value posted to the blockchain; later that user can prove that the document existed at that moment in time by hashing the document and comparing it
  - Useful for situations where data needs to be proven to exist at a specified time, such as with prior art claims

A Platform for Research

- The development systems are not constrained
- Researchers can interact with others (e.g., not alone)
- Researchers do not need to spend real money to experiment
- Researchers will be freely available to:
  - Utilize any blockchain available
  - Utilize any development tool necessary

Internal NIST Topics of Interest

- Inter-Chain research – between multiple blockchains
- Side-Chain research – blockchains spun off of blockchains
- Off-Chain research – between a blockchain and an off-chain database
- Providing immutable data sources within areas where there are accusations of tampering after the fact
- Identity Management
- Smart Contracts

Challenges with Blockchain Technology

- Perception of the technology – Use of Bitcoin for illegal means has generated specific reputations for the entire technology
- Lack of interoperability – currently blockchains are mostly technological silos
- Limited transaction size – large transactions lead to massive blockchain sizes; a lot of data is stored “off chain” and becomes another piece of data to manage
- Not Simple – it is actually multiple complicated technologies combined

Challenges with Blockchain Technology

- Data Immutability – how to deal with data which cannot be changed?
- Proof of work is expensive – computationally, and power consumption
- Relatively new – a lot of technology and development tools around blockchains is still in alpha or beta level
- Small number of research workbenches like this, where researchers can explore the technology freely

Questions?

- Thank You!
- Contact:
  - dylan.yaga@nist.gov