

Blockchain and Distributed Ledger Technologies: Opportunities, Challenges and Future Work

Andrew Regenscheid
Cryptographic Technology Group



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

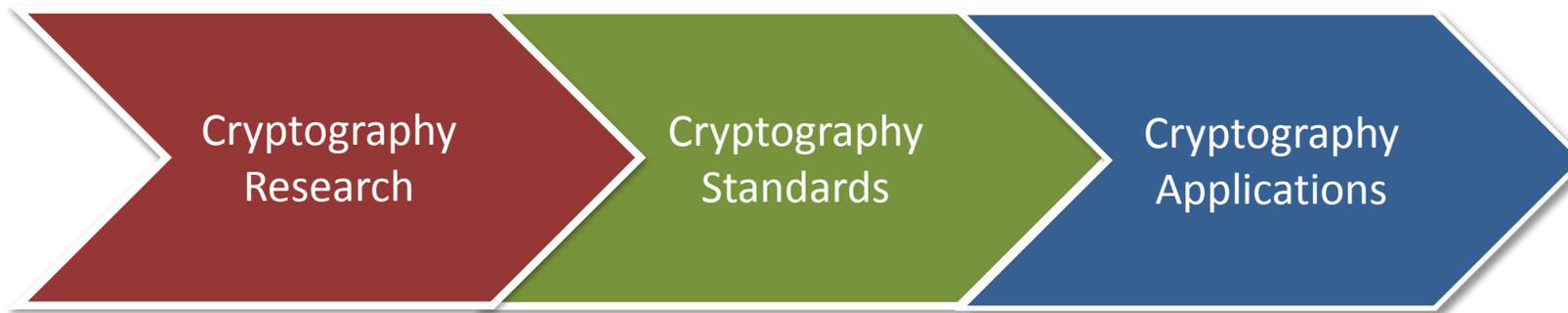
Cryptographic Technology Group

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.



Blockchain is...

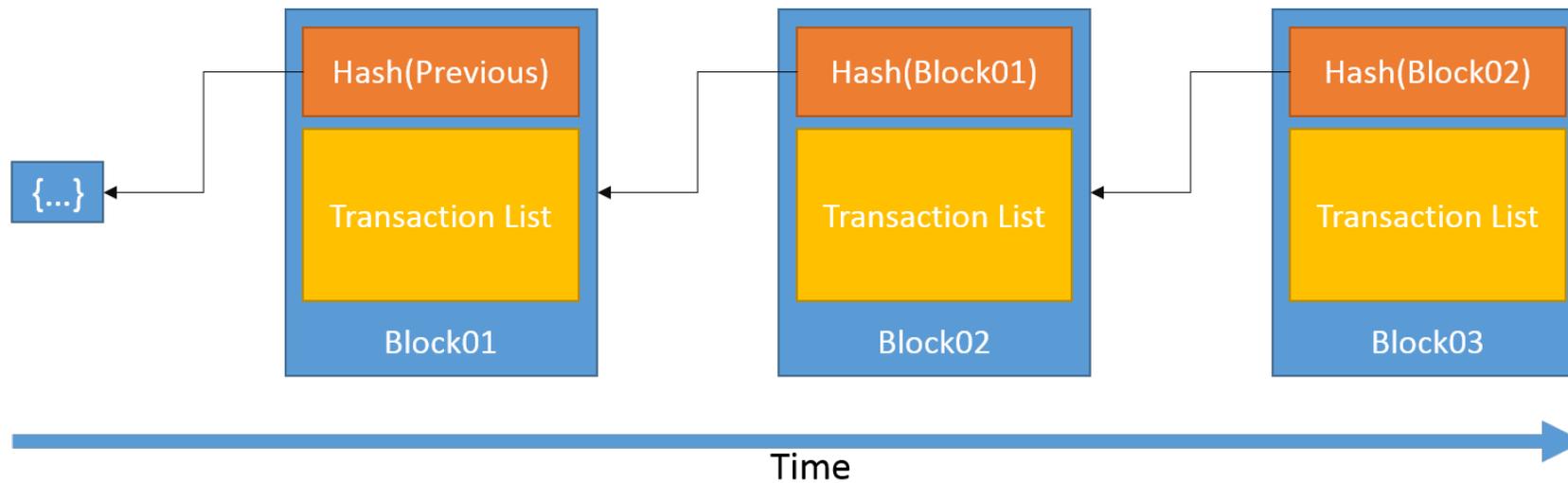
A **distributed ledger** which is:

- *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

NIST Blockchain Workbench

dylan.yaga@nist.gov

NIST/ITL/CSD

Security Components and Mechanisms Group

6.28.2017

NIST

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

MultiChain Explorer - Mozilla Firefox

MultiChain Explorer x NIST/ITL/CSD Blockchain x Ethereum Block Explorer x +

localhost:2750

MultiChain Explorer NIST/ITL/CSD Blockch... Ethereum Block Expl...

MultiChain Explorer

Search by address, block number or hash, transaction or chain name:

Address or hash search requires at least the first 6 characters.

Status	Chain	Blocks	Transactions	Assets	Addresses	Streams	Peers	Started	Age (days)
Connected	MultiChain multichain-private-permissioned	103	109	0	4	1	4	2017-06-15	11.0

Latest Transactions

Txid	Type	Confirmation	Time
51ed34a6d29c6c3416d3123d96b4ad4f256274b29fd38bf52753e6c99820da2b	Permissions	11 confirmations	10 days
de06a50cf068bd276486b65a39daae99cf318a1403468a897b26ef49eec3cb73	Permissions	22 confirmations	10 days
519662b49002a1b4196180e4663b6215dc8ddf2b5582543e8dea36990a7bf697	Permissions	33 confirmations	10 days
d94f2a3f9fadd323a144cb73b170577ba1bbd71766dca9f3c6b4a0788570ff45	Permissions	44 confirmations	10 days
acf01d52bf0d6c751fe3bc96e4198632c875edd1e882b4a1a1b7a8e9500ce960	Metadata	103 confirmations	10 days

Powered by MultiChain Explorer

Workbench – Demo Application

The screenshot shows a Mozilla Firefox browser window with the title "NIST/ITL/CSD Blockchain Workbench - Mozilla Firefox". The address bar displays "localhost/multichain-private-permissioned/index.php". The browser tabs include "MultiChain Explorer", "NIST/ITL/CSD Blockchain", and "Ethereum Block Explorer". The page features a navigation menu with "Home", "Blockchain Addresses", "Blockchain Info", and "Contact". The main content area has two tabs: "Post Text" (selected) and "Post File Hash". Below the tabs is a form with three input fields: "To Address" (text input with value "1kRb9yv61tGQ6GmUpRTyTeux8Vd1rcRVkUws"), "From Address" (dropdown menu with value "1kRb9yv61tGQ6GmUpRTyTeux8Vd1rcRVkUws"), and "Blockchain Input" (text input). A blue "Submit" button is located below the "Blockchain Input" field. A red asterisk and the text "* Required Field" are positioned below the "Submit" button. On the left side of the browser window, a vertical sidebar contains several application icons, including a gear, a globe, a folder, a magnifying glass, a document, a person, a Bitcoin logo, and a DVD icon.

Workbench – Ethereum Explorer

ETHER EXPLORER Home Blockchain Info

Tx Hash, Address, or

Tx Hash, Address, or Block # Search

Current Block: 66709

ETH/USD Price: \$284.87

Gas Limit: 4,712,388 m/s

Block Time: 2 second(s)

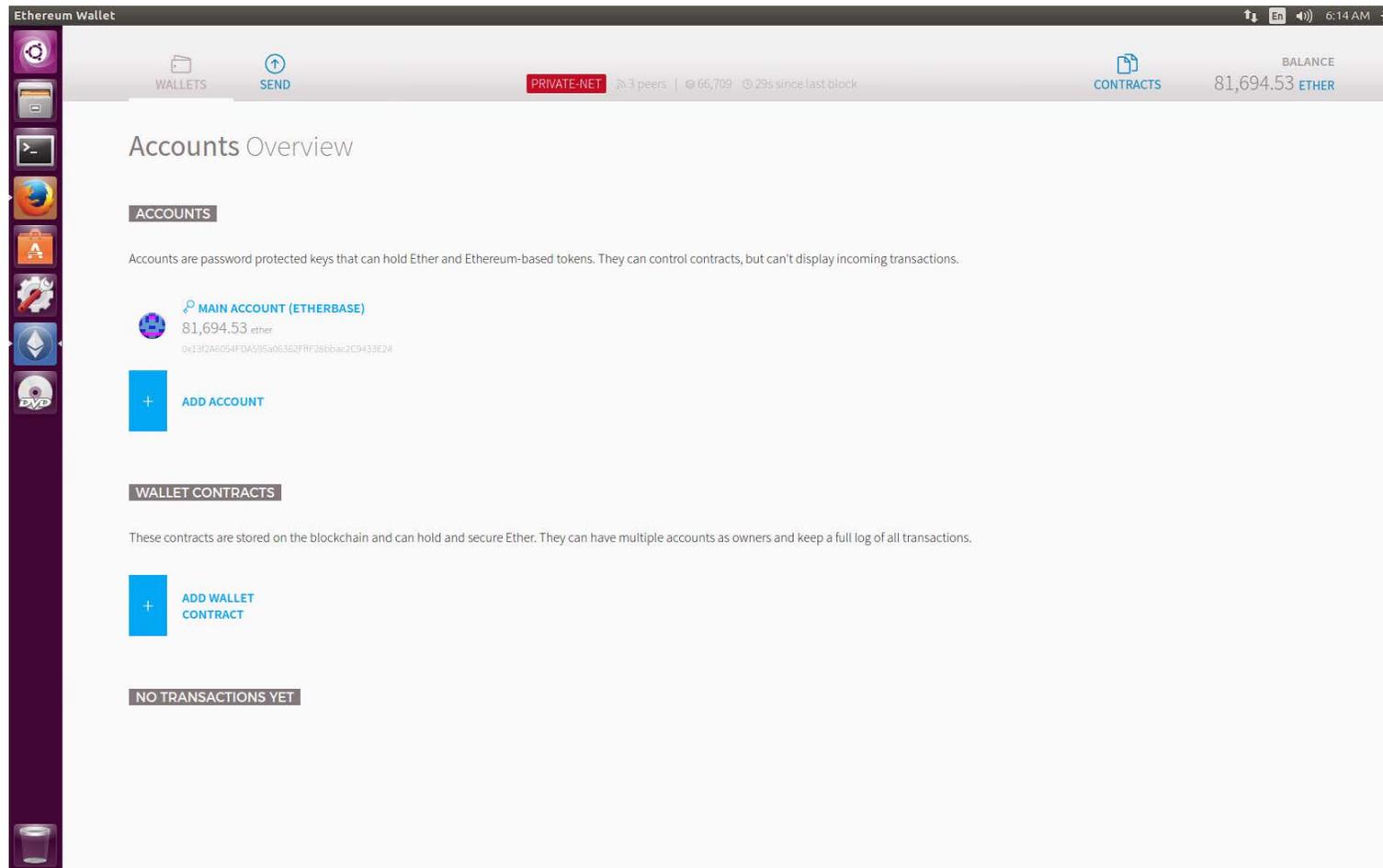
Current Diff.: 0.000 T

Hashrate: 54.254 TH/s

Recent Blocks Most Recent Blocks in the Ethereum Network

Block #	Block Hash	Difficulty	Miner	Size	Date	# of TXs	Gas used
66709	0x51d668f...	0.000 T	0x6405e2b71bcf681692d0a4317b035e6e4bee403e	0.538 kB	Jun 26, 2017 6:13:44 AM	0	0 m/s
66708	0x71e4499...	0.000 T	0xa0cb7b09afa614c2d79702564094e1660911f3f2	0.538 kB	Jun 26, 2017 6:13:42 AM	0	0 m/s
66707	0x49a6d5e...	0.000 T	0x6405e2b71bcf681692d0a4317b035e6e4bee403e	0.538 kB	Jun 26, 2017 6:13:38 AM	0	0 m/s
66706	0x1e1aa3a...	0.000 T	0xa0cb7b09afa614c2d79702564094e1660911f3f2	0.538 kB	Jun 26, 2017 6:13:17 AM	0	0 m/s
66705	0xdfcfd4...	0.000 T	0x01f568c5afa293cf821b0c9c02e3cce354e93c9d	0.538 kB	Jun 26, 2017 6:12:25 AM	0	0 m/s
66704	0x1bfa400...	0.000 T	0x01f568c5afa293cf821b0c9c02e3cce354e93c9d	0.538 kB	Jun 26, 2017 6:12:20 AM	0	0 m/s
66703	0xfcc00a...	0.000 T	0x6405e2b71bcf681692d0a4317b035e6e4bee403e	0.538 kB	Jun 26, 2017 6:11:56 AM	0	0 m/s
66702	0x9f36d71...	0.000 T	0x01f568c5afa293cf821b0c9c02e3cce354e93c9d	0.538 kB	Jun 26, 2017 6:11:39 AM	0	0 m/s
66701	0x5a86562...	0.000 T	0x13f2a6054fda595a06362ffff28bbac2c9433e24	0.538 kB	Jun 26, 2017 6:11:28 AM	0	0 m/s
66700	0x7cb7e9b...	0.000 T	0x6405e2b71bcf681692d0a4317b035e6e4bee403e	0.538 kB	Jun 26, 2017 6:11:00 AM	0	0 m/s

Workbench – Ethereum Mist Wallet



Workbench Deliverables

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

```
1  #!/bin/bash
2  #####
3  #Script: setup_multichain_private_permissioned.sh
4  #Purpose: To Download, Setup & Configure, Launch MultiChain Blockchain Platform,
5  #         Blockchain Explorer, and associated Web Demos for the NIST/IIL/CSD
6  #         Internal Blockchain Workbench
7  #Tested On: Ubuntu 16.04 Server & Desktop
8  #Author: Dylan Yaga
9  #Email: dylan.yaga@nist.gov
10 #
11 #
12 #####
13
14 #Variables
15 #####
16 #Variables that can be changed to alter the names of the blockchain
17 blockchain_name=multichain-private-permissioned
18 web_folder=/var/www/html/${blockchain_name}
19 explorer_name=${blockchain_name}-explorer
20 blockchain_folder=/home/${USER}/${blockchain_name}
21 explorer_folder=${blockchain_folder}/multichain-explorer/multichain-explorer-maste
22 #Boolean to determine whether or not to use the embedded base64 webpage
23 use_embedded=true
24 #resources
25 use_embedded=true
26 #####
```

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