[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Blockchain: Clarifying the Hope from the Hype

Eliezer Kanal

Technical Manager, CERT

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Copyright 2018 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

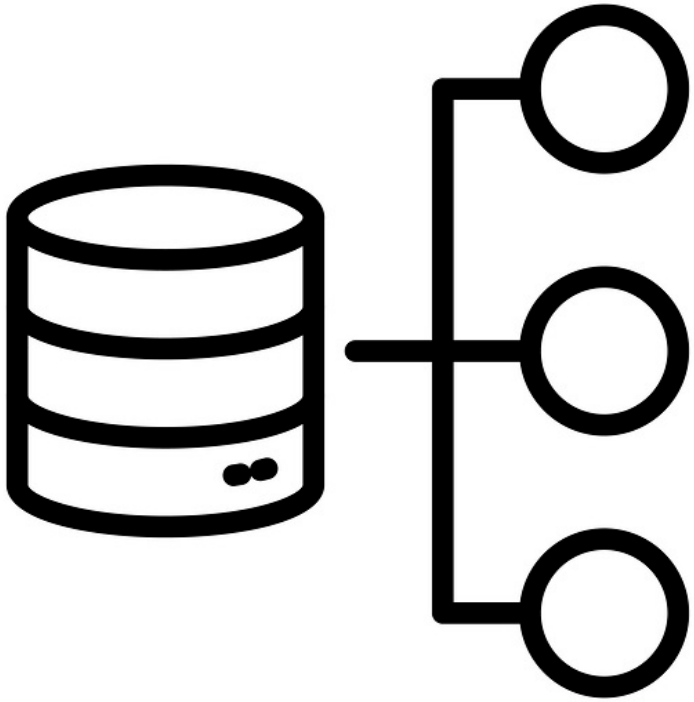
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM18-0205

Previous models of computing



Data Storage:

Database

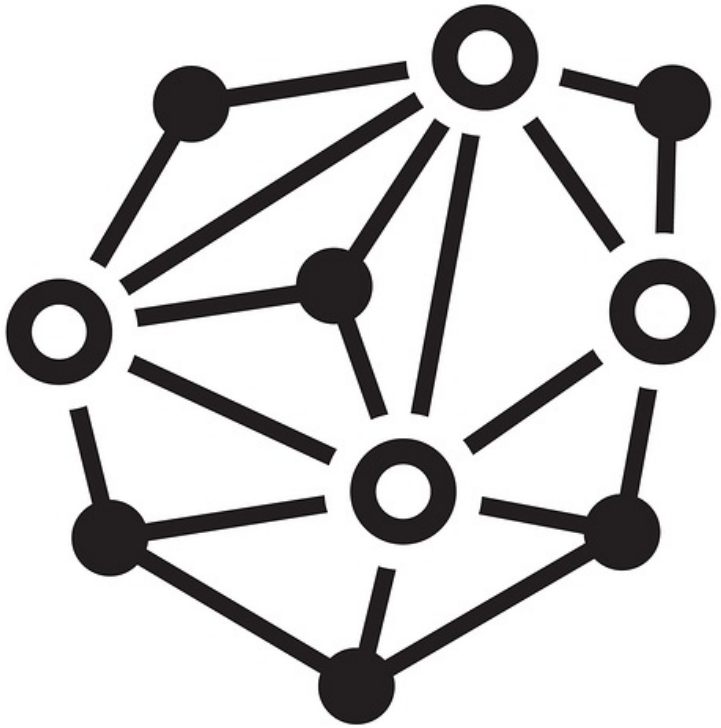
Program Execution:

Local

© 2018 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Blockchain



Data Storage:

Blockchain or Network

Program Execution:

Network

© 2018 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

There’s more!

Data on the chain cannot be removed

Identity fundamentally linked to activity

Easily auditable

Mediates untrusted party interactions

© 2018 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Bitcoin

Based on blockchain technology

Does two things:

1. Maintains a distributed ledger
2. Enables transactions

Mining determines transaction timing

© 2018 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Bitcoin

Block #509169

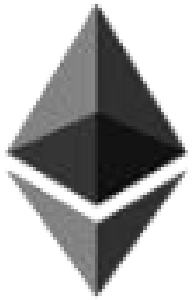
Summary	
Number Of Transactions	1915
Output Total	10,289.28130284 BTC
Estimated Transaction Volume	1,818.68925455 BTC
Transaction Fees	0.4893378 BTC
Height	509169 (Main Chain)
Timestamp	2018-02-14 15:16:59
Received Time	2018-02-14 15:16:59
Relayed By	58COIN
Difficulty	2,874,674,234,415.94
Bits	392292856
Size	1132.416 kB
Weight	3992.574 kWU
Version	0x20000000
Nonce	1858980081
Block Reward	12.5 BTC

Hashes	
Hash	00000000000000000002c4b94355945eea353bc720c58a73c2b8593f489550cb3
Previous Block	00000000000000000001d620a2e3ad126ec5038bf42343c419eb6fcdf7240a471
Next Block(s)	
Merkle Root	3ad680735c45cc62b1ea6b7efeb34f82a2660c5e8280354c45f7ffa03c9137e2

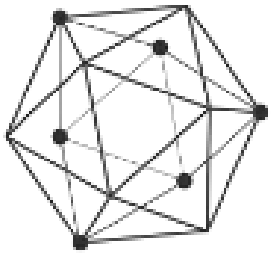
Transactions

ab0da64ea834fd2acb81eb081d8103c9e31fd14a7d055f2ce2718c59dd4fa5df			2018-02-14 15:16:59
No Inputs (Newly Generated Coins)	→	14DjTuAUh87cwRsbU1z6W8hZY6FnEkpfLS Unable to decode output address	12.9893378 BTC 0 BTC
			12.9893378 BTC

4feb8981da942b10a2a384003fba1c1d78c8f192cd2747e43ae552ed237f267d			2018-02-14 15:16:59
1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP	→	12PaHiRJBmvJYmTpZ32Pswf8eYbKcAE131 1GpqR4vsdvEfgtNyiUrDrfDLTBJvnsentX 1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP	0.4983 BTC 0.1495 BTC 5.01651602 BTC
			5.66431602 BTC



ethereum



HYPERLEDGER

© 2018 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Ethereum

Block 5089469

Previous | Next

Hash:	0x4b7ced1ac95fa07a06fbb0352468797bd038e8c1fb0f6d4de2838f5712469c27
Difficulty:	2,863,007,803,096,150
Miner:	✔ miningpoolhub1 (0xb293...) (Mined in 19s)
Reward:	3.13573 ETH | $2,777.29 (Block Reward: 3 ETH + Fee Reward: 0.13573 ETH + Uncle Inclusion Reward: 0 ETH)
Tx Fees:	0.13573 ETH | $120.22 (4.33% of the total block reward)
Tx / Uncles:	202 Transactions and 0 Uncles
Gas Limit:	8,000,029
Gas Usage:	83.8 % (6,701,815 of 8,000,029)
Lowest Gas Price:	1 GWei
Time:	02/14/2018 10:31:12 AM (a minute ago)
Size:	28,742 bytes
Extra	t3 (Raw: 0x7433)

202 Transactions | 0 Uncles | Details

Hash	Type	From	To	Value	Fee	Gas Price
0x00622dc883...	Tx	0x5BaEac0a0417a...	0x342DB8C17dF30...	0.03175 ETH	0.0021 ETH	100 GWei
0x2f21a28b88...	Tx	0x96b7DA642FAA7...	0xee4d84B1E8C78...	0.01 ETH	0.00208 ETH	99 GWei
0x4a6a150361...	Tx	✔ Bittrex (0xfbb1...)	0x419D0d8BdD9aF...	0 ETH	0.00531 ETH	90 GWei
↳	Call	0x419D0d8BdD9aF...	0x267808e5246D1...	0 ETH	0.0028 ETH	90 GWei
↳	Call	0x267808e5246D1...	0xe6a51Bd48f93A...	0 ETH	0.00247 ETH	90 GWei
0x7359bb70de...	Tx	0x45a0ba49c5244...	0xAA1A6e3e6EF20...	4.97698 ETH	0.00233 ETH	70 GWei

Use cases abound

Payment System

Health Care Records

Real Estate Records

© 2018 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Use Cases Abound

1. **Financial Instruments, Records and Models**
    1. Currency
    2. Private equities
    3. Public equities
    4. Bonds
    5. Derivatives (futures, forwards, swaps, options and more complex variations)
    6. Voting rights associated with any of the above
    7. Commodities
    8. Spending records
    9. Trading records
    10. Mortgage / loan records
    11. Servicing records
    12. Crowd-funding
    13. Micro-finance
    14. Micro-charity
2. **Public Records**
    1. Land titles
    2. Vehicle registries
    3. Business license
    4. Business incorporation / dissolution records
    5. Business ownership records
    6. Regulatory records
    7. Criminal records
    8. Passports
    9. Birth certificates
    10. Death certificates
    11. Voter IDs
    12. Voting
    13. Health / Safety Inspections
    14. Building permits
    15. Gun permits
    16. Forensic evidence
    17. Court records
    18. Voting records
    19. Non-profit records
    20. Government/non-profit accounting/transparency
3. **Private Records**
    1. Contracts
    2. Signatures
    3. Wills
    4. Trusts
    5. Escrows
    6. GPS trails (personal)
4. **Other Semi-Public Records**
    4. Degree
    5. Certifications
    6. Learning Outcomes
    7. Grades
    8. HR records (salary, performance reviews, accomplishment)
    9. Medical records
    10. Accounting records
    11. Business transaction records
    12. Genome data
    13. GPS trails (institutional)
    14. Delivery records
    15. Arbitration
5. **Physical Asset Keys**
    1. Home / apartment keys
    2. Vacation home / timeshare keys
    3. Hotel room keys
    4. Car keys
    5. Rental car keys
    6. Leased cars keys
    7. Locker keys
    8. Safety deposit box keys
    9. Package delivery (split key between delivery firm and receiver)
    10. Betting records
    11. Fantasy sports records (!)
6. **Intangibles (?)**
    1. Coupons
    2. Vouchers
    3. Reservations (restaurants, hotels, queues, etc)
    4. Movie tickets
    5. Patents
    6. Copyrights
    7. Trademarks
    8. Software licenses
    9. Videogame licenses
    10. Music/movie/book licenses (DRM)
    11. Domain names
    12. Online identities
    13. Proof of authorship / Proof of prior art
7. **Other**
    1. Documentary records (photos, audio, video)
    2. Data records (sports scores, temperature, etc)
    3. Sim Cards
    4. GPS network identity
    5. Gun unlock codes
    6. Weapons unlock codes
    7. Nuclear launch codes (!)
    8. Spam control (micro-payments for posting)

© 2018 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Opportunities

Architecture stack difficult to manage

Programming blockchains is difficult, mistakes costly

Compatibility with existing systems?

Many still investigating

© 2018 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Contact Information

Eliezer Kanal

Technical Manager & Principle Researcher

Telephone: +1 412.268.5204

Email: ekanal@sei.cmu.edu

© 2018 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.