Proof-of-Publication Using the Bitcoin Blockchain

Prof. Christopher E. Wilmer
Managing Editor of Ledger
University of Pittsburgh
Overview:

1. What is *Ledger*? (and what is a cryptocurrency?!) 
2. Who’s involved with *Ledger*? 
4. Proof-of-publication using blockchain technology
What is *Ledger*?

- A peer-reviewed journal for publishing original research on cryptocurrency-related subjects
What is *Ledger*?

- A peer-reviewed journal for publishing original research on cryptocurrency-related subjects
What is a cryptocurrency?

• You may have heard of something called Bitcoin
• Bitcoin is a cryptocurrency
What is a cryptocurrency?

- You may have heard of something called Bitcoin
- Bitcoin is a cryptocurrency
- In many ways it is like any other currency (e.g., USD, Yen, Euros) but where some functions that traditionally rely on trusted authorities are replaced by the use of clever cryptography

Examples:
- Sending money to someone via check/wire/online
- Controlling the money supply
What is a cryptocurrency?

- You may have heard of something called Bitcoin
- Bitcoin is a cryptocurrency
- In many ways it is like any other currency (e.g., USD, Yen, Euros) but where some functions that traditionally rely on trusted authorities are replaced by the use of clever cryptography

- Examples:
  - Sending money to someone via check/wire/online
  - Controlling the money supply
- Bitcoin is decentralized (no single point of failure)
- There is no Bitcoin company or person who controls/manages it... it just exists autonomously (like a language... or a virus)
What is a cryptocurrency?

- Cryptocurrencies, despite their name, are not just about money
- They are about recording ownership of arbitrary data and facilitating the transfer of ownership to someone else without a central institution
What is a cryptocurrency?

- Cryptocurrencies, despite their name, are not just about money
- They are about recording ownership of arbitrary data and facilitating the transfer of ownership to someone else without a central institution

- Examples:
  - Trading stocks without a stock exchange
  - Transferring the title to a house without a notary/court
  - Filing a patent without a patent office
  - Issuing concert tickets without a ticket office
What is a cryptocurrency?

- Cryptocurrencies, despite their name, are not just about money
- They are about recording ownership of arbitrary data and facilitating the transfer of ownership to someone else without a central institution
- Examples:
  - Trading stocks without a stock exchange
  - Transferring the title to a house without a notary/court
  - Filing a patent without a patent office
  - Issuing concert tickets without a ticket office
  - Timestamping scientific results/publications (more on that later)
Who invented Bitcoin?

• In 2008, someone using the pseudonym Satoshi Nakamoto published a paper describing Bitcoin (not in a journal!)
• After stimulating some discussion among cryptographers Satoshi released a working prototype in 2009
Who invented Bitcoin?

- In 2008, someone using the pseudonym Satoshi Nakamoto published a paper describing Bitcoin (not in a journal!)
- After stimulating some discussion among cryptographers Satoshi released a working prototype in 2009
- The currency units, “bitcoins,” were worthless for the first two years... then token trades started (bitcoins for pizza)
- Now 6 years later, it is a $\textbf{16 billion economy}$, each of the $\sim 16$ million bitcoins is worth over $1,000+$ USD
Broader Interest

• Since Bitcoin, thousands of similar cryptocurrencies have been created with tweaks to the underlying technology

• “Blockchain technology” = cryptocurrency (for all practical purposes)
Broader Interest

- Since Bitcoin, thousands of similar cryptocurrencies have been created with tweaks to the underlying technology
- “Blockchain technology” = cryptocurrency (for all practical purposes)
- Princeton, Stanford, MIT, Duke University, and several others teach Bitcoin/Blockchain courses now
- Bank of England, DTCC, and other large institutions have created blockchain “strategy” or “think-tank” groups
- Multiple US federal and state level hearings
Broader Interest

- Since Bitcoin, thousands of similar cryptocurrencies have been created with tweaks to the underlying technology
- “Blockchain technology” = cryptocurrency (for all practical purposes)
- Princeton, Stanford, MIT, Duke University, and several others teach Bitcoin/Blockchain courses now
- Bank of England, DTCC, and other large institutions have created blockchain “strategy” or “think-tank” groups
- Multiple US federal and state level hearings
- National Science Foundation (NSF) has already funded over $3 million for cryptocurrency research
- Nearly 1,000 papers published on the subject
Problem: No good scholarly venue

- Growth in research papers* significant, but very little peer-review and highly scattered (forums, pre-publication archives, disparate journals)

*Academic, and quasi-academic research papers, journal articles, and theses related to Bitcoin
Problem: No good scholarly venue

- For many academics, their research on cryptocurrency doesn’t “count” in the eyes of their peers unless it is published in a traditional academic journal
- We wanted to make it easier for academics to get involved in cryptocurrency research
Problem: No good scholarly venue

- For many academics, their research on cryptocurrency doesn’t “count” in the eyes of their peers unless it is published in a traditional academic journal
- We wanted to make it easier for academics to get involved in cryptocurrency research
- We also wanted to raise the standard of research being done by scholars (not necessarily academics) already in the Bitcoin/cryptocurrency community
Problem: No good scholarly venue

- For many academics, their research on cryptocurrency doesn’t “count” in the eyes of their peers unless it is published in a traditional academic journal
- We wanted to make it easier for academics to get involved in cryptocurrency research
- We also wanted to raise the standard of research being done by scholars (not necessarily academics) already in the Bitcoin/cryptocurrency community
- So we set out to create a traditional academic journal devoted to this topic: *Ledger* (name is derived from yet another synonym for “blockchain technology” → “distributed ledger technology”)

NFAIS 2017: *Ledger*
Traditional academic journal?

- Some members of the community wanted to leverage cryptocurrencies to create a futuristic decentralized “journal” for cryptocurrency research
Traditional academic journal?

- Some members of the community wanted to leverage cryptocurrencies to create a futuristic decentralized “journal” for cryptocurrency research
- In principle, advanced cryptocurrencies like Ethereum could (probably) allow for an entirely decentralized journal publishing platform
- Citation tracking, in particular, is well suited to be done in a decentralized way using a cryptocurrency
Traditional academic journal?

- Some members of the community wanted to leverage cryptocurrencies to create a futuristic decentralized “journal” for cryptocurrency research
- In principle, advanced cryptocurrencies like Ethereum could (probably) allow for an entirely decentralized journal publishing platform
- Citation tracking, in particular, is well suited to be done in a decentralized way using a cryptocurrency

- We chose to leave all of that to someone else
What is *Ledger*?

- The first peer-reviewed journal for publishing original research on cryptocurrency-related subjects
- Founded in 2015
What is *Ledger*?

- The first peer-reviewed journal for publishing original research on cryptocurrency-related subjects
- Founded in 2015
- Broad scope:
  - Mathematics, cryptography, engineering, computer science
  - Law, economics, finance, social sciences
What is *Ledger*?

- The first peer-reviewed journal for publishing original research on cryptocurrency-related subjects
- Founded in 2015
- Broad scope:
  - Mathematics, cryptography, engineering, computer science
  - Law, economics, finance, social sciences
- Open access
  - Free to view content (no subscription cost)
  - Free to publish (no author fees)
What is Ledger?

• The first peer-reviewed journal for publishing original research on cryptocurrency-related subjects
• Founded in 2015
• Broad scope:
  o Mathematics, cryptography, engineering, computer science
  o Law, economics, finance, social sciences
• Open access
  o Free to view content (no subscription cost)
  o Free to publish (no author fees)
• Published by the University Library System at the University of Pittsburgh
What is *Ledger*?
• We had our first call for papers Sept. 2015 for the inaugural issue, which came out Dec. 2016.
• It was well publicized:
What is *Ledger*?

- We had our first call for papers Sept. 2015 for the inaugural issue, which came out Dec. 2016.
- It was well publicized:

  "...Bitcoin officially came of age in academia with the launch of *Ledger*, the first journal dedicated to cryptocurrency research."

Retweet from Gavin Andresen:

MIT Media Lab @medialab · Sep 19
Ledger, the first #cryptocurrency-focused academic journal, has posted its first call for papers [mitsha.re/Sp9Rr](http://mitsha.re/Sp9Rr)

Retweet from Chris Dixon:

(200,000+ followers)

"*Ledger* is a peer-reviewed scholarly journal on cryptocurrency and blockchain technologies. [ledgerjournal.org/ojs/index.php/...]

*Ledger* is a peer-reviewed scholarly journal that publishes full-length original research articles on the subjects of cryptocurrency and blockchain technology, as well as any relevant intersections with mathematics, computer science, engineering, law, and economics. It is published online on a quarterly basis by the University Library System, University of Pittsburgh.
Who’s involved with Ledger?

Editorial Board:

**Economics**
- Dr. Michael Kumhof
  - Bank of England

**Comp. Sci.**
- Prof. William Knottenbelt
  - Imperial College London

**Cryptocurrency**
- Prof. William Knottenbelt
  - Imperial College London

**Math**
- Prof. Christopher Douglas
  - Oxford University

**Econ.**
- Dr. Catherine Mulligan
  - Imperial College London

**Law**
- Prof. Jerry Brito
  - Coin Center

**Business**
- Prof. George Giaglis
  - Athens Uni. of Econ. & Business

**Finance**
- Prof. Campbell Harvey
  - Duke University

**Business + CS**
- Dr. Catherine Mulligan
  - Imperial College London

**Chem + CS**
- Prof. Vijay Pande
  - Stanford University

**Comp. Sci.**
- Prof. Srini Devadas
  - MIT

**Elec-Eng + CS**
- Prof. Houman Shadab
  - New York Law School

**Economics**
- Mr. Jon Matonis
  - Bitcoin Foundation

**Comp.Sci., CS = Computer Science**
Who’s involved with Ledger?

Managing Editors

Prof. Christopher Wilmer
University of Pittsburgh

Dr. Peter Rizun
Physicist/Entrepreneur

Dr. Shin’ichiro Matsuo
CELLOS Consortium

Prof. Tim Peterson
Harvard University

Dr. Primavera De Filippi
Harvard Law School

Mr. Andrew Miller
U. Maryland

Mr. Antony Zegers
Defence R&D

Prof. Charles W. Evans
Barry University

Dr. Patrick Deegan
CTO Personal Blackbox

Mr. Richard Ford Burley
Boston College

Dr. Tim Peterson
Harvard University

Dr. Primavera De Filippi
Harvard Law School

Mr. Kieren Scott James-Lubin
UC Berkeley

Mr. Antony Zegers
Defence R&D

Prof. Charles W. Evans
Barry University

Dr. Patrick Deegan
CTO Personal Blackbox

Mr. Kieren Scott James-Lubin
UC Berkeley

Prof. Aaron Wright
Cardozo Law
Publishing in Ledger: Policies & workflow

- Similarities to most journals
  - Three article types: original research, reviews, and perspectives
  - Editors handle submissions, find and contact reviewers (typically 3), make final decisions
  - Single-blind review process (reviewers know identity of author but not the other way around)
  - Multiple review rounds if necessary
Publishing in Ledger: Policies & workflow

- Differences from most journals
  - Transparent review process: Reviews, including author correspondence, are published alongside accepted article
Publishing in in Ledger: Policies & workflow

• Differences from most journals
  o Transparent review process: Reviews, including author correspondence, are published alongside accepted article
  o Once accepted, articles are digitally signed by the authors (we provide a user-friendly tool for this)
    ➢ Cryptographically proves article has not been altered
Publishing in Ledger: Policies & workflow

• Differences from most journals
  o Transparent review process: Reviews, including author correspondence, are published alongside accepted article
  o Once accepted, articles are digitally signed by the authors (we provide a user-friendly tool for this)
    ➢ Cryptographically proves article has not been altered
  o The signed document is timestamped by the Bitcoin blockchain
    ➢ Cryptographically proves article existed before certain time
Publishing in in Ledger: Policies & workflow

- Differences from most journals
  - Transparent review process: Reviews, including author correspondence, are published alongside accepted article
  - Once accepted, articles are digitally signed by the authors (we provide a user-friendly tool for this)
    - Cryptographically proves article has not been altered
  - The signed document is timestamped by the Bitcoin blockchain
    - Cryptographically proves article existed before certain time
  - Under exceptional circumstances, authors may publish under a pseudonym
    - Demand less than anticipated. One pseudonymous cryptographer, whose research was on how to make an even more anonymous version of Bitcoin, decided to publish with us under his real name
Authors can digitally sign their papers, *Ledger* will timestamp the file hash in the Blockchain.

LEDGER timestamps hash in Blockchain (proof of existence)

You can also verify a signature to someone’s *real name* if they use OneName!

Authors can digitally sign their papers, *Ledger* will timestamp the file hash in the Blockchain.

LEDGER timestamps hash in Blockchain (proof of existence)

You can also verify a signature to someone’s *real name* if they use OneName!

Authors can digitally sign their papers, *Ledger* will timestamp the file hash in the Blockchain.

LEDGER timestamps hash in Blockchain (proof of existence)

You can also verify a signature to someone’s *real name* if they use OneName!

Authors can digitally sign their papers, *Ledger* will timestamp the file hash in the Blockchain.

LEDGER timestamps hash in Blockchain (proof of existence)

You can also verify a signature to someone’s *real name* if they use OneName!

Authors can digitally sign their papers, *Ledger* will timestamp the file hash in the Blockchain.

LEDGER timestamps hash in Blockchain (proof of existence)

You can also verify a signature to someone’s *real name* if they use OneName!

Authors can digitally sign their papers, *Ledger* will timestamp the file hash in the Blockchain.

LEDGER timestamps hash in Blockchain (proof of existence)

You can also verify a signature to someone’s *real name* if they use OneName!

Authors can digitally sign their papers, *Ledger* will timestamp the file hash in the Blockchain.

LEDGER timestamps hash in Blockchain (proof of existence)

You can also verify a signature to someone’s *real name* if they use OneName!

Authors can digitally sign their papers, *Ledger* will timestamp the file hash in the Blockchain.

LEDGER timestamps hash in Blockchain (proof of existence)

You can also verify a signature to someone’s *real name* if they use OneName!

Authors can digitally sign their papers, *Ledger* will timestamp the file hash in the Blockchain.

LEDGER timestamps hash in Blockchain (proof of existence)

You can also verify a signature to someone’s *real name* if they use OneName!
Proof-of-Publication using Blockchain Technology

- Blockchains as a data-storage mechanism, are well suited to be used in scholarly publishing because:
Proof-of-Publication using Blockchain Technology

- Blockchains as a data-storage mechanism, are well suited to be used in scholarly publishing because:
  - Extremely resilient, tamper-proof, practically indestructible database
Proof-of-Publication using Blockchain Technology

• Blockchains as a data-storage mechanism, are well suited to be used in scholarly publishing because:
  • Extremely resilient, tamper-proof, practically indestructible database
  • No single point of failure
Proof-of-Publication using Blockchain Technology

- Blockchains as a data-storage mechanism, are well suited to be used in scholarly publishing because:
  - Extremely resilient, tamper-proof, practically indestructible database
  - No single point of failure
  - No cost of operation
Proof-of-Publication using Blockchain Technology

- Blockchains as a data-storage mechanism, are well suited to be used in scholarly publishing because:
  - Extremely resilient, tamper-proof, practically indestructible database
  - No single point of failure
  - No cost of operation
  - Incontrovertible proof of publication date, even across countries and institutions whose incentives are not aligned
Proof-of-Publication using Blockchain Technology

• Blockchains as a data-storage mechanism, are well suited to be used in scholarly publishing because:
  • Extremely resilient, tamper-proof, practically indestructible database
  • No single point of failure
  • No cost of operation
  • Incontrovertible proof of publication date, even across countries and institutions whose incentives are not aligned

(which is sometimes a point of contention for scientists racing to discover cure/new theorem/etc.)
The End