June 10, 2020

IP Opportunities and Pitfalls in Protecting Blockchain Technology

Charles R. Macedo, Esq.

Isabella Ortiz, Esq.

AMSTER ROTHSTEIN & EBENSTEIN LLP
Intellectual Property Law

Northwestern | INVO
Innovation and New Ventures

A webinar presentation specially prepared for
The Association of University Technology Managers (AUTM) Foundation

1

AMSTER ROTHSTEIN & EBENSTEIN LLP
Intellectual Property Law

Blockchain Technology IP Opportunities and Pitfalls

Agenda

1. Understanding What is Blockchain Technology
2. Determining What To Patent In The Blockchain Stack
3. Obtaining Patents That Cover Evolving Technology In The Blockchain Space
4. Making A Patent
5. Gathering Information

2

AMSTER ROTHSTEIN & EBENSTEIN LLP
Intellectual Property Law

Blockchain Technology IP Opportunities and Pitfalls

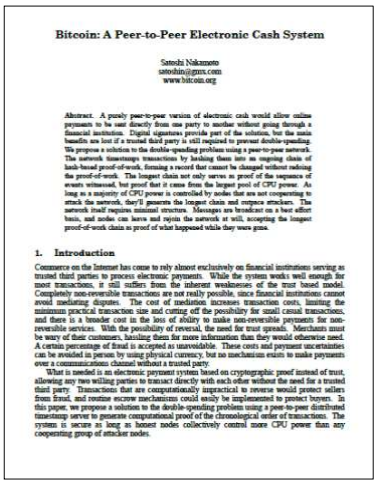
Agenda

1. Understanding What is Blockchain Technology

autm

3

In 2009, Satoshi Nakamoto published
"Bitcoin: A Peer-to-Peer Blockchain System"



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

Under the pseudonym "Satoshi Nakamoto" a whitepaper was published introducing Bitcoin and its Peer-to-Peer Blockchain technology.

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm

4

In 2009, Satoshi Nakamoto published "Bitcoin: A Peer-to-Peer Blockchain System"

"Bitcoin: A Peer-to-Peer Blockchain Cash System"

Commerce on the Internet has come to rely almost exclusively on financial institutions serving **as trusted third parties** to process electronic payments. While the system works well enough for most transactions, it still suffers from **the inherent weaknesses of the trust based model**. **Completely non-reversible transactions are not really possible**, since financial institutions cannot avoid mediating disputes. **The cost of mediation increases transaction costs**, limiting the minimum practical **transaction size** and cutting off the possibility **for small casual transactions**, and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, **hassling them for more information** than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make **payments over a communications channel without a trusted party.**

The Technical Problems Sought to be Solved By Bitcoin Version of Blockchain

"Inherent weakness of the trust based model":

- Reversibility of transactions
- Transaction costs of mediating disputes
- No small transactions
- Need for personal information
- Physical cash can't be transmitted over a communication channel

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm

5

In 2009, Satoshi Nakamoto published "Bitcoin: A Peer-to-Peer Blockchain System"

"Bitcoin: A Peer-to-Peer Blockchain Cash System"

What is needed is an **electronic payment system** based on **cryptographic proof instead of trust**, allowing any two willing parties to transact directly with each other **without the need for a trusted third party**. Transactions that are **computationally impractical to reverse would protect sellers from fraud**, and **routine escrow mechanisms could easily be implemented to protect buyers**. In this paper, we propose a solution to the double-spending problem **using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions**. The system is secure as long as **honest nodes collectively control more CPU power than any cooperating group of attacker nodes**.

The Technical Solution Offered By Bitcoin Version of Blockchain

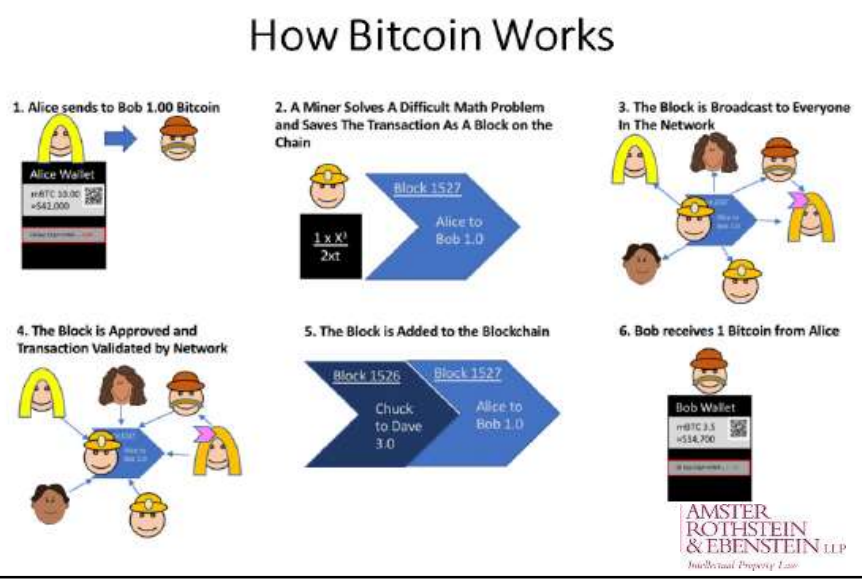
"What is needed is electronic payment system based on cryptographic proof instead of trust":

- No trusted third party
- Computationally impractical to reverse
- Routine escrow mechanisms to protect against fraud
- Peer-to-peer distributed timestamp server to generate computational proof of chronological order of transactions
- Requiring majority control of CPU power to protect against attack

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm

6

How the Bitcoin Blockchain Works



AMSTER ROTHSTEIN & EBENSTEIN LLP
Intellectual Property Law

autm

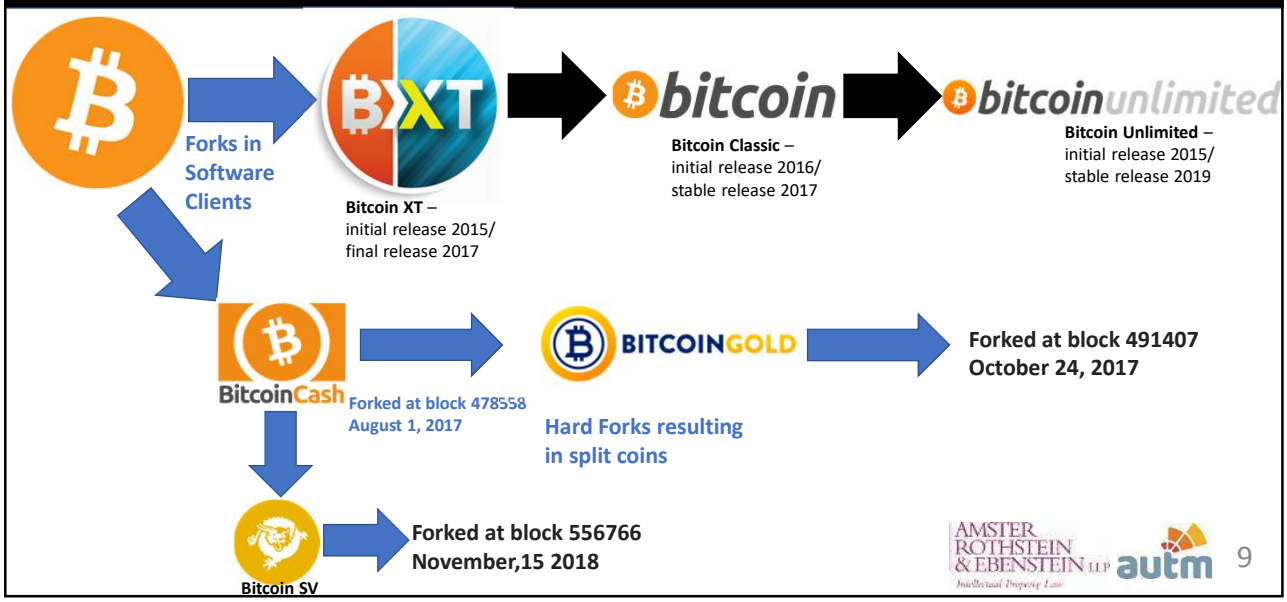
How the Bitcoin Blockchain Works

Key Elements/Aspects of Bitcoin Blockchain:

1) **Authentication Mechanism:** Uses Public Key-Private Key Cryptography to Authenticate Transactions
2) **Consensus Mechanism:** Proof of Work (Bitcoin, Litecoin, etc.)
3) **Peer-to-Peer Network:** Open and Transparent Network
4) **Version Control:** Majority of Computing Power Adopts Protocol (This results in forks)
5) **Block Authentication:** Each Block is tied to earlier blocks mathematically
6) **Timing of Blocks:** Every 10 minutes

AMSTER ROTHSTEIN & EBENSTEIN LLP
Intellectual Property Law
autm

"Forks" in Bitcoin Inspired Other Bitcoin Like Blockchains



AMSTER ROTHSTEIN & EBENSTEIN LLP autm 9

"Clones" in Bitcoin Also Inspired Other Bitcoin Like Blockchains

Bitcoin spinoff in 2011 – Quicker block time

Bitcoin spinoff in 2011 – stores data in transactions

AMSTER ROTHSTEIN & EBENSTEIN LLP autm 10

Alternative Protocols Have Been Developed (and continue to be developed)

Monero

Offers hidden and shielded wallets

Ethereum

Introduces Smart Contracts and Tokens

Ripple

For Fast Cheap Money Transfer

Hyperledger

Formed by the *Linux foundation*, and many other partners such as *IBM*, *Intel*, *SAP*, *Cisco*, *Daimler*, and *American Express*, to design and develop enterprise blockchains

libra

Facebook's effort to introduce a new blockchain and stable coin

Filecoin

A peer-to-peer file storage system

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm 11

Smart Contracts, DApps and Tokens Are Being Built on Underlying Blockchains

Ethereum

Ethereum is a cryptocurrency and blockchain platform that provides a decentralized, global computer on which developers can build decentralized Apps (DApps) and their own crypto tokens.

GEMINI dollar

An ERC233 standard stablecoin issued and operated by Gemini.

Maker

An ERC20 token that grants holders a vote on changes in the Maker Protocol, thereby manage the financial risks of Dai

Bread

An ERC20 standard token used to pay for services in a Bread wallet.

Golem

An ERC20 token used to pay for services on the Golem decentralized cloud computing network.

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm 12

AMSTER ROTHSTEIN & EBENSTEIN LLP
Intellectual Property Law

Blockchain Technology IP Opportunities and Pitfalls

Agenda

2. Determining What To Patent In The Blockchain Stack

autm

13

The Blockchain Stack

The Protocol (software code) is the foundation of a blockchain stack. It is the software run by all the participants on the network the defines how transactions occur.

e.g.,

- Bitcoin Protocol,
- Litecoin Protocol,
- Ethereum Protocol,
- Zcash Protocol,
- etc.

Protocol (Software Code)

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm 14

The Blockchain Stack

The protocol is built to run on a wide variety of **computer systems**.

e.g.,
- Nodes (administrator computers),
- Miners,
- clients (wallets),
- custodial systems.
- etc.

Computer Systems Running Protocol

Protocol (Software Code)

The Blockchain Stack

The blockchain creates coins or a **crypto-currency** which is generally available to be exchanged in the peer-to-peer network

e.g.,
- Bitcoin,
- Litecoin,
- Ethereum,
- Zcash,
- etc.

Crypto-Currency

Computer Systems Running Protocol

Protocol (Software Code)

The Blockchain Stack

Messages/Embedded Code/Smart Contracts
Crypto-Currency
Computer Systems Running Protocol
Protocol (Software Code)

The blockchain is a giant database that keeps track of ownership and transfer of coins and crypto-currency. In addition, **other data and code** (smart contracts) can also be tracked.

e.g.,

- Bitcoin Messages,
- CryptoKitties Software,
- Gemini Dollar Smart Contract,
- etc.

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm 17

The Blockchain Stack

Tokens
Messages/Embedded Code/Smart Contracts
Crypto-Currency
Computer Systems Running Protocol
Protocol (Software Code)

Tokens are a top layer "coin" like way in which smart contracts keep track of information. Tokens can be used and traded like Crypto-currency, but often are the subject of more elaborate rules governed by smart contracts.

e.g.,

- Gas,
- Gemini Dollar,
- Pre-sale of inventory,
- etc.

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm 18

The Blockchain Stack

Tokens	e.g., Gas, Gemini Dollar, Pre-sale of inventory, etc.
Messages/Embedded Code/Smart Contracts	e.g., Bitcoin Messages, CryptoKitties Software, Gemini Dollar Smart Contract, etc.
Crypto-Currency	e.g., Bitcoin, Litecoin, Ethereum, Zcash, etc.
Computer Systems Running Protocol	e.g., Nodes (administrator computers), Miners, clients (wallets), custodial systems. etc.
Protocol (Software Code)	e.g., Bitcoin Protocol, Litecoin Protocol, Ethereum Protocol, Zcash Protocol, etc.

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm 19

Off Ramps

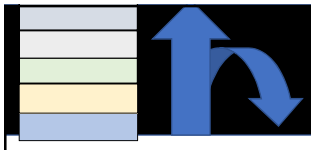
Businesses have been developed by modifying the original bitcoin protocol or by developing new protocols

Protocol (Software Code)

e.g.,

- LiteCoin protocol – modifies timing of blocks
- Ethereum protocol – provides for smart contracts
- ZCash protocol – provides for shielded wallets
- AiCoin protocol – provides for a private blockchain
- Blockstack protocol – provides a new ecosystem to develop and run decentralized apps

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm 20



Off Ramps

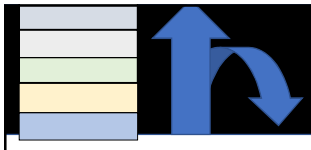
Businesses have developed by improving **computer systems** or **software associated with computer systems** for running protocols

e.g.,
- New ASICs for Mining,
- Mining Consortiums,
- Better Wallets,
- Custodial Systems,
- etc.

Computer Systems Running Protocol

Protocol (Software Code)

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm 21



Off Ramps

Businesses develop with new coins and systems and methods that interact with such coins.

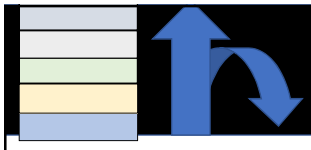
e.g.,
- New Coins (like Litecoin, Ether, ZCash),
- Inventory Control Systems (Whopper coins),
- Exchanges (Gemini) Store & Transfer Value,
- Financial Products (ETP/Options/Futures),
- Side Chains
- Etc.

Crypto-Currency

Computer Systems Running Protocol

Protocol (Software Code)

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm 22



Off Ramps

Businesses develop by embedding messages or code in immutable blockchain transactions.

Messages/Embedded Code/Smart Contracts

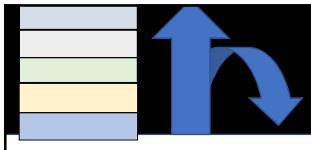
Crypto-Currency

Computer Systems Running Protocol

Protocol (Software Code)

e.g.,
- Convey Info (sending messages in bitcoin transaction)
- Share Pictures,
- Use smart contracts to make Stable Coins (Gemini Dollar),
- electronic Contracts and electronic Securities,
- Oracles
- Side Chains
- Dapps
- Etc.

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm 23



Off Ramps

Businesses have developed by issuing new **"tokens"** to reflect stored value, anticipated future value, or transfer value.

Tokens

Messages/Embedded Code/Smart Contracts

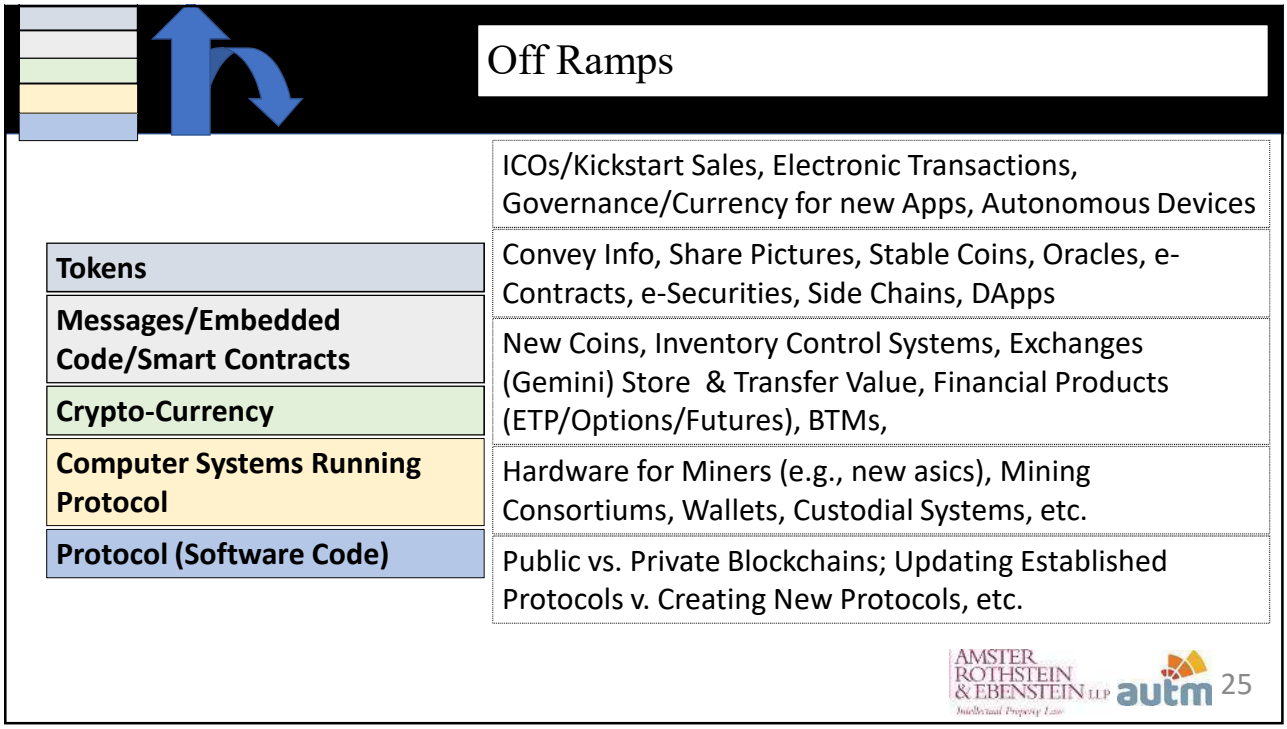
Crypto-Currency

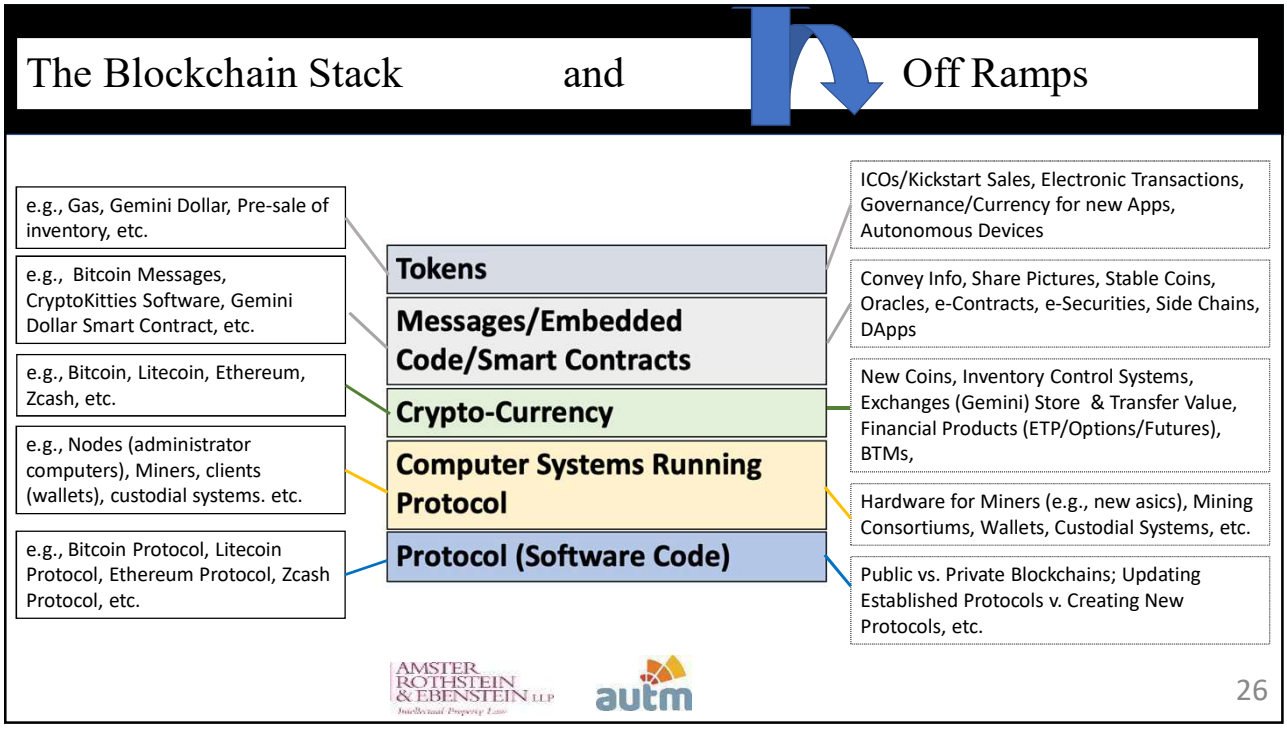
Computer Systems Running Protocol

Protocol (Software Code)

e.g.,
- Initial Coin Offerings (ICO's) used to raise funds pre-launch/Kickstart Sales,
- Electronic Transactions,
- Autonomous Devices can transact in tokens using smart contracts
- Providing governance or currency for other apps
- Etc.

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm 24


Off Ramps
Tokens
Messages/Embedded Code/Smart Contracts
Crypto-Currency
Computer Systems Running Protocol
Protocol (Software Code)
ICOs/Kickstart Sales, Electronic Transactions, Governance/Currency for new Apps, Autonomous Devices
Convey Info, Share Pictures, Stable Coins, Oracles, e-Contracts, e-Securities, Side Chains, DApps
New Coins, Inventory Control Systems, Exchanges (Gemini) Store & Transfer Value, Financial Products (ETP/Options/Futures), BTMs,
Hardware for Miners (e.g., new asics), Mining Consortiums, Wallets, Custodial Systems, etc.
Public vs. Private Blockchains; Updating Established Protocols v. Creating New Protocols, etc.
AMSTER ROTHSTEIN & EBENSTEIN LLP
autm
25


The Blockchain Stack
and
Off Ramps
e.g., Gas, Gemini Dollar, Pre-sale of inventory, etc.
e.g., Bitcoin Messages, CryptoKitties Software, Gemini Dollar Smart Contract, etc.
e.g., Bitcoin, Litecoin, Ethereum, Zcash, etc.
e.g., Nodes (administrator computers), Miners, clients (wallets), custodial systems. etc.
e.g., Bitcoin Protocol, Litecoin Protocol, Ethereum Protocol, Zcash Protocol, etc.
Tokens
Messages/Embedded Code/Smart Contracts
Crypto-Currency
Computer Systems Running Protocol
Protocol (Software Code)
ICOs/Kickstart Sales, Electronic Transactions, Governance/Currency for new Apps, Autonomous Devices
Convey Info, Share Pictures, Stable Coins, Oracles, e-Contracts, e-Securities, Side Chains, DApps
New Coins, Inventory Control Systems, Exchanges (Gemini) Store & Transfer Value, Financial Products (ETP/Options/Futures), BTMs,
Hardware for Miners (e.g., new asics), Mining Consortiums, Wallets, Custodial Systems, etc.
Public vs. Private Blockchains; Updating Established Protocols v. Creating New Protocols, etc.
AMSTER ROTHSTEIN & EBENSTEIN LLP
autm
26

Applications

- Cyber Security
- Financial Services
- Healthcare
- Internet of Things
- Cross Border Payments
- Retail
- Supply Chain
- Identity Credentials
- Voting
- Insurance
- Cloud Storage
- Property and Land Titles
- Government
- Smart Contracts

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm 27

Major Advancements

SUPPLY CHAIN
Walmart and IBM blockchain initiative to help track their food supply. The system has been used to track millions of packages containing about 20 different food products, and perform more than 100,000 traces of their origins.

HEALTHCARE
Insurance claims can be processed faster now with smart contracts.

RETAIL
Jewelry industry (De Beers) can trace where your diamonds were mined from by tracing the stones from the point they are minded right up to the point when they are sold to consumers.

SMART CONTRACTS
Licenses for services and music can be created at a faster and easier rate.

PROPERTY AND LAND TITLE
Escrow process and commission rates of purchasing property will soon be eliminated through smart contracts. (i.e. Deedcoin).

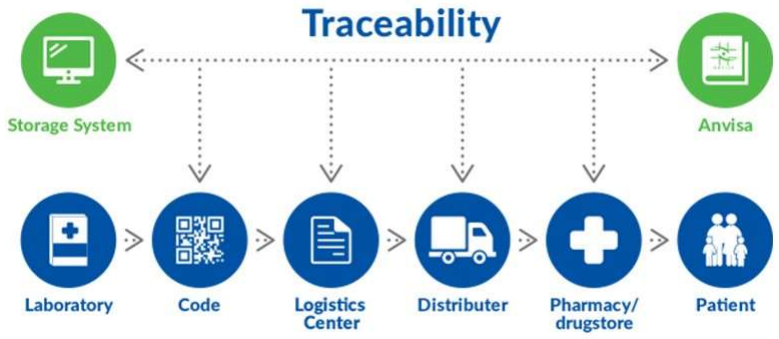
VOTING
Voter registrations and verification would increase the amount of legitimate votes and access to voting online.

CLOUD STORAGE
Startups now have a way to pitch to investors live in a secure manner. Entrepreneurs create summaries of their products or services and investors can quickly sort and find potential opportunities. (Pitch Ventures)

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm 28

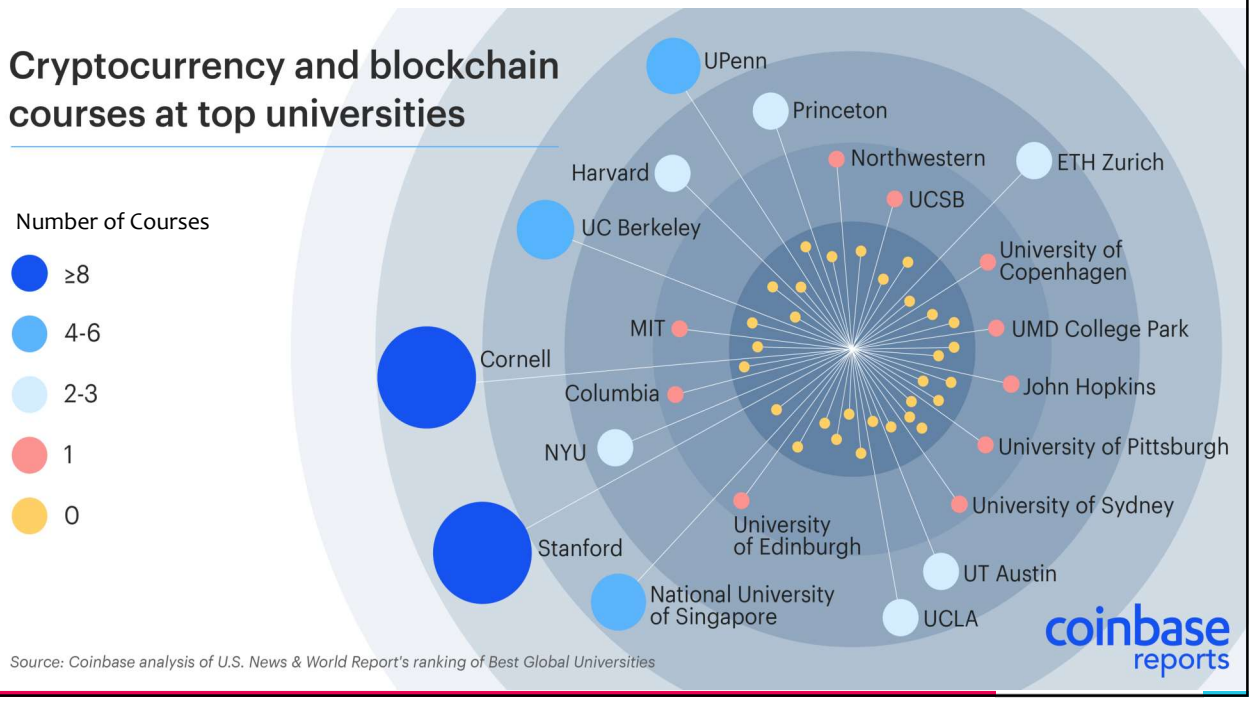
Healthcare

1. Insurance Claims
2. Record Keeping
3. Fundraising for New R&D
4. Financing Commercial Real Estate
5. Professional Investment
6. Supply Chain Tracking
7. Improving Financial Wellness in the Health Care Business



AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law
autm
29

Cryptocurrency and blockchain courses at top universities

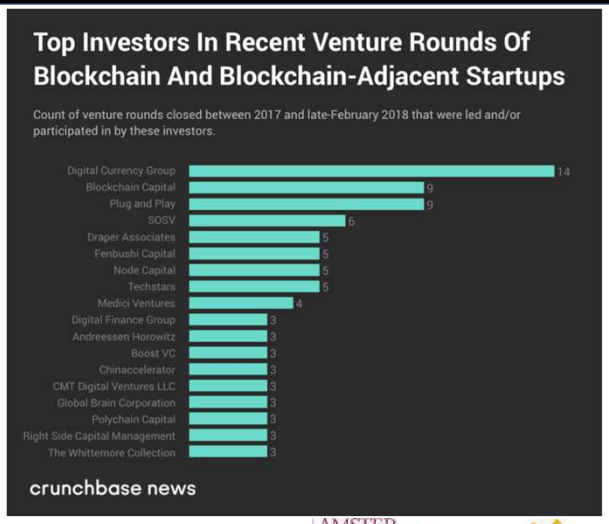


Source: Coinbase analysis of U.S. News & World Report's ranking of Best Global Universities

coinbase reports

Future of Investing in Blockchain

- The blockchain hype and the early days of the internet have many similarities.
- Venture capitalists have tripled their investment in blockchain and crypto related firms
- Blockchain will be able to provide near-instantons settlements
- Trading costs should decrease
- Greater transparency and trust because of distributed ledgers
- Regulators are beginning to realize the benefits of attracting blockchain startups



AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm 31

Types of Investment in Blockchain: Initial Coin Offering vs. Venture Capital Funding

Raising Money
- Venture Capital Funding
  - Raising money from a group of venture capitalists, who will risk their own money in exchange for company equity.
- ICO
  - Raising money worldwide from anyone having Internet and enough money to buy a token.
  - Allows startups to fund themselves without any equity commitment

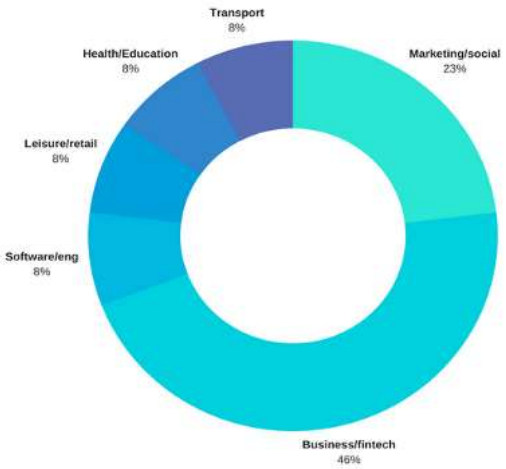
Goals
- Venture Capital Funding
  - Consulting, business guidelines, scalability, connection to industry influencers, proof of concept.
- ICO
  - Quick way to raise money with as many people involved as possible, creating a stronger community.

Audience
- Venture Capital Funding
  - Experienced businessmen, having a lot to propose and demand. Great for a superb idea but lacking a demo, white paper, smooth pitch, roadmap
- ICO
  - Everybody from everywhere. No working prototype needed.
  - Quick buy process

Requirements
- Venture Capital Funding
  - Strong staff, working product, share part of company
- ICO
  - No formal requirements yet, you decide what and how your token holders will get in exchange for their money

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm 32

Startup by Industry



ICO

- In 2018, $7.8 billion was raised through ICOs
- In 2019, ICO's went down from previous years
- 45% were successful.
- Ethereum is success story of an ICO

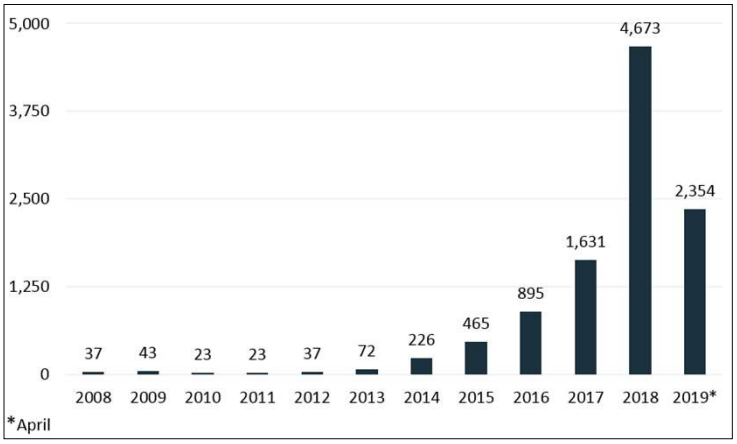
Venture Capital

- VC Investment reached 2.8 billion in 2019 from 807 separate deals that were tied to crypto and blockchain technology.
- Institutions are becoming more comfortable putting their capital into the space, while angel investors are "falling off", which shows a sign of the industry maturing.
- One reason for the decline in funding is that many products are still trying to find product market fit.

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm 33

Blockchain Filings

Blockchain Patent Applications Per Year



Statistics Current as of April 2019, mined from Iplytics Platform Database (https://www.iplytics.com/)
Also available at: https://www.iam-media.com/who-are-patent-leaders-blockchain

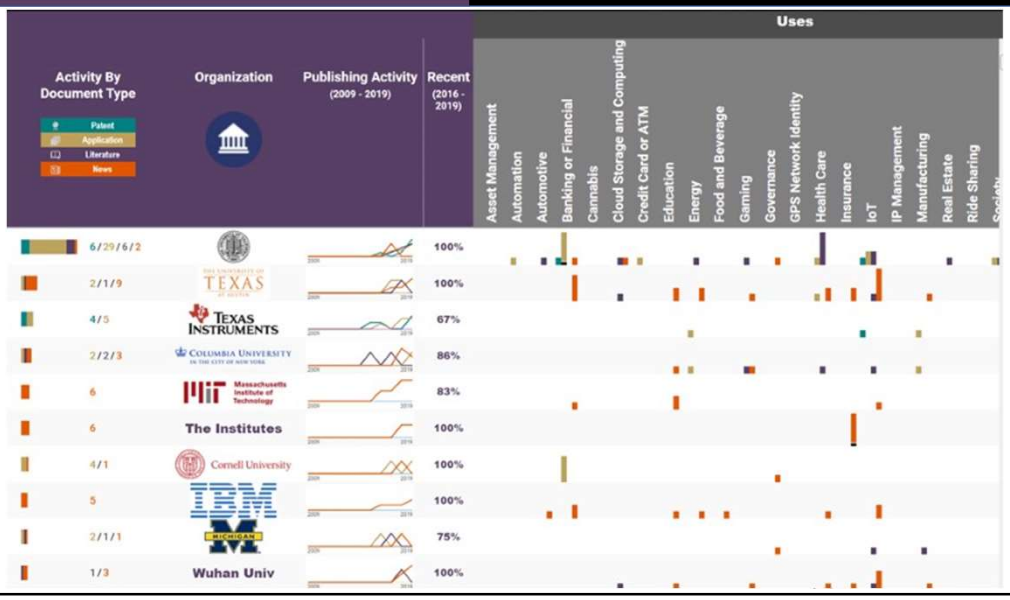
AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law 34

Intellar

Blockchain IP & Technology Landscape

Patents & Apps US/EP/PCT/JP/KR/CN (Q1 2010 - Q3 2019)
Global literature & news (Q1 2015 - Q3 2019)

University Activity



https://perceptionpartners.com/intellar-library-landscape-dashboard-products/blockchain-landscape-competitive-intelligence-dashboard

35

AMSTER ROTHSTEIN & EBENSTEIN LLP
Intellectual Property Law

Blockchain Technology IP Opportunities and Pitfalls

Agenda

3. Obtaining Patents That Cover Evolving Technology In The Blockchain Space

autm

36

Patent Evolving Technology

Blockchain Technology is always evolving and disclosure needs to cover variations what might be considered key attributes:

- Public Blockchains → Private Blockchains → Hybrid Chains
- Proof of Work Consensus → Proof of Stake and other Consensus Mechanisms
- Sending Messages → Smart contracts and Tokens → DApps
- Public and Transparent Data → Shielded Wallets
- Blockchains → Merkle Trees
- Fungible Coins → Nonfungible tokens

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm 37

Patent Evolving Technology

Public Blockchains → Private Blockchains

Public Blockchain

Semi-Private Blockchain

Private Blockchain

HYPERLEDGER

corda

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm 38

Patent Evolving Technology

Proof of Work Consensus Mechanisms → Proof of Stake and other Consensus Mechanisms

Proof of Work

Proof of Stake

Byzantine Fault

libra

Proof of Capacity

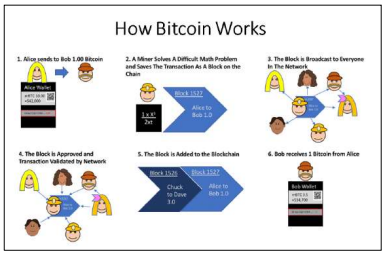
BURST

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm 39

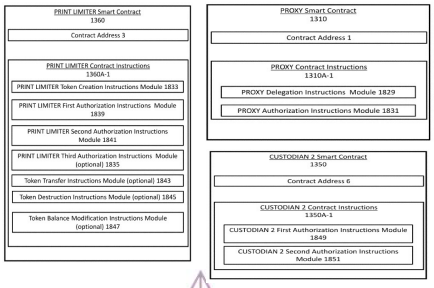
Patent Evolving Technology

Sending Messages → Smart contracts and Tokens

Sending Messages



Smart Contracts



Tokens

GEMINI dollar

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm 40

Patent Evolving Technology

Public and Transparent Data → Shielded Wallets

Public and Transparent Data

Shielded Wallets

Zcash

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm 41

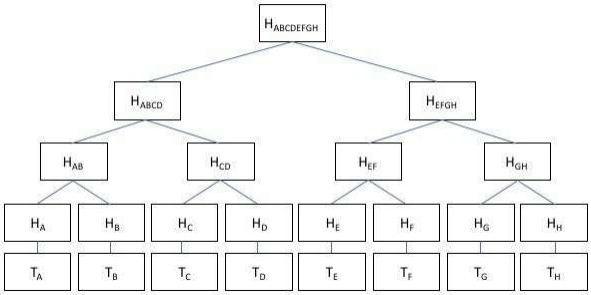
Patent Evolving Technology

Blockchains → Merkle Trees

Blockchain

- **Tokens**
- **Messages/Embedded Code/Smart Contracts**
- **Crypto-Currency**
- **Computer Systems Running Protocol**
- **Protocol (Software Code)**

Merkle Tree



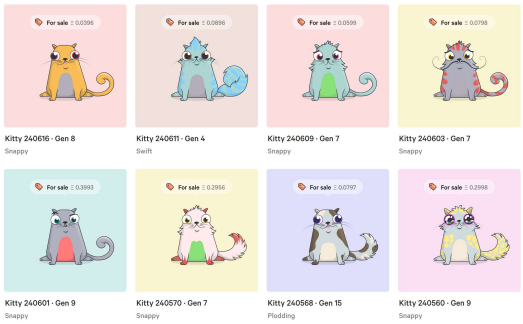
AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm 42

Patent Evolving Technology

Fungible Coins → Nonfungible tokens

Fungible Coins

Non-Fungible Tokens



AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm

43

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law

Agenda

autm

Blockchain Technology IP Opportunities and Pitfalls

4. Making A Patent

44

Making A Patent

CONSIDERATIONS FOR PATENTING BLOCKCHAIN TECHNOLOGY

What should be considered when patenting Blockchain?

- Patent Eligibility (35 U.S.C. § 101)
- Divided Infringement
- Sufficient Disclosure (35 U.S.C. § 112)

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm 45

Making A Patent

PATENT APPLICATION

Specification

Specification should include discussions of:

- Technical Problem and Technical Solution
- Sample Pseudo Code showing this is a computer based technology

Figures

Figures should show:

- Topology of Network
- Components of computers and associated electronic devices
- Process flow charts

Claims

Claims (and specification) should:

- Meaningfully tie invention to blockchain technology
- Claim interaction with blockchain – e.g., sending messages to blockchain
- Detail is important
- Have claim include some action beyond storing information

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm 46

Making A Patent

Stable Value Coin Patent – USP 10,373,158

Exemplary Pseudo Code

Table 5 illustrates embodiments of code which uses LockRequestable in a template consistent with embodiments of the present invention.

TABLE 5

```
contract C is ..., LockRequestable {
  struct PendingAction {
  t v;
  ...
  }
  address public custodian;
  mapping (bytes32 => PendingAction) public pendingActionMap;
  function C(address _custodian, ...) public {
    custodian = _custodian;
    ...
  }
  modifier onlyCustodian
    require(msg.sender == custodian);
    ...;
  }
  function requestAction(t_v, ...) public returns (bytes32 lockId) {
    require(_v != 0);
    lockId = generateLockId( );
    pendingActionMap[lockId] = PendingAction({
    v: _v,
    ...
    });
    emit ActionLocked(lockId, _v, ...);
  }
  function confirmAction(bytes32 _lockId) public onlyCustodian {
    PendingAction storage pendingAction = pendingActionMap[_lockId];
    t v = pendingAction.v;
    require(v != 0);
    ... // copy any other data from pendingAction
    delete pendingActionMap[_lockId];
    ... // execute the action
    emit ActionConfirmed(_lockId, v, ...);
  }
  event ActionLocked(bytes32 _lockId, t_v, ...);
  event ActionConfirmed(bytes32 _lockId, t_v, ...);
}
```

Exemplary Problem and Solution

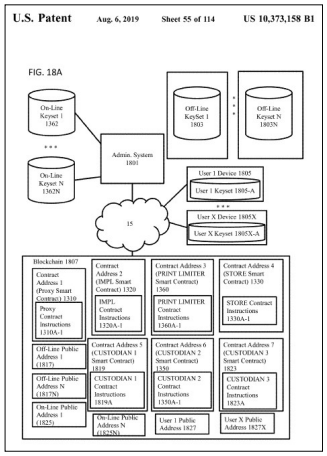
In embodiments, custodianship of the proxy and store also grants exclusive power to pass custodianship to a new instance of Custodian. Thus, one of the technical computer problems associated with the immutability of ERC20 smart contracts on the Ethereum blockchain has been solved, thus allowing for a self-upgrade of custodianship. In embodiments, since a set of signers for a given instance of a Custodian is fixed, a change to the off-line keyset may be implemented instead having a current Custodian authorize itself to be replaced by a new instance of Custodian with a new set of signers.

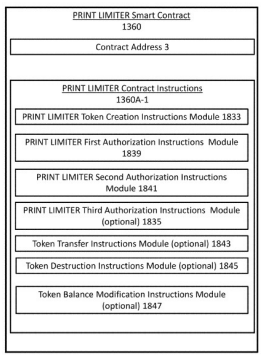
AMSTER ROTHSTEIN & EBENSTEIN LLP autm Intellectual Property Law 47

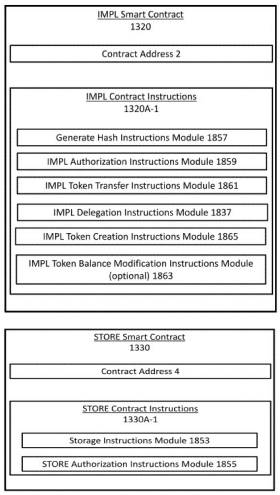
Making A Patent

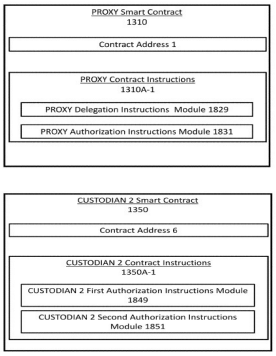
Stable Value Coin Patent – USP 10,373,158

Exemplary Network and Component Figures









AMSTER ROTHSTEIN & EBENSTEIN LLP autm Intellectual Property Law 48

Making A Patent

Stable Value Coin Patent – USP 10,373,158

Exemplary Network and Component Figure

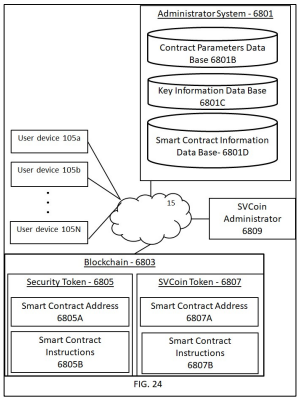


FIG. 24

Exemplary Graphical User Interface Figure

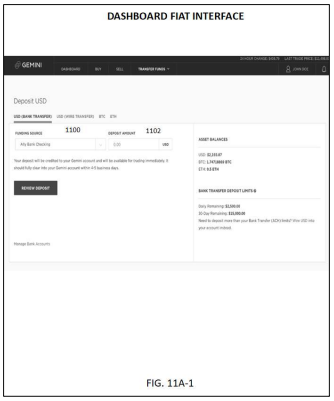
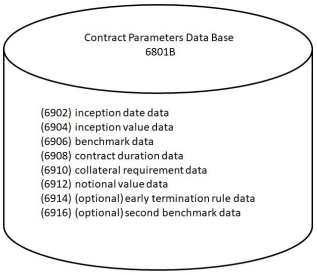


FIG. 11A-1

Exemplary Component Figure



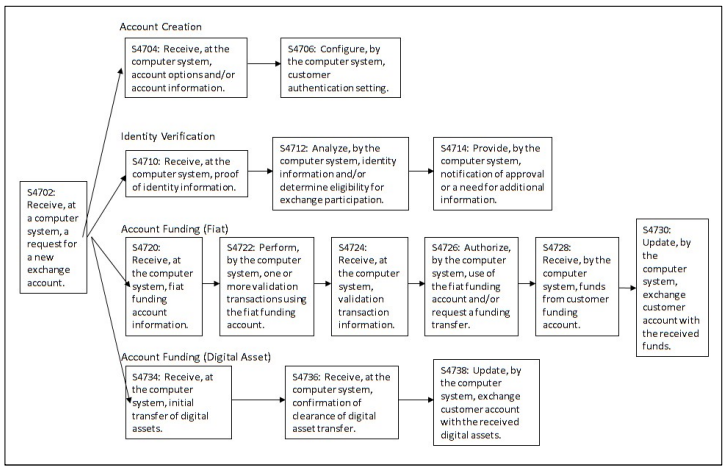
AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm

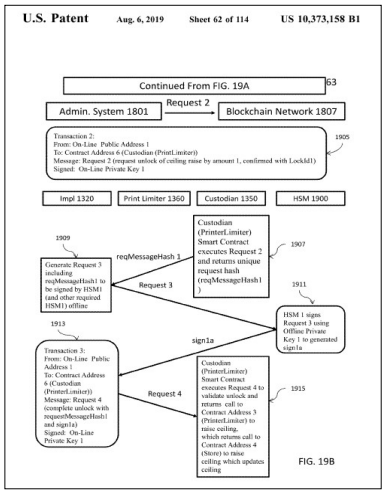
49

Making A Patent

Stable Value Coin Patent – USP 10,373,158

Exemplary Process Flows From Server Perspective





AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law

50

AMSTER ROTHSTEIN & EBENSTEIN LLP
Intellectual Property Law

Blockchain Technology IP Opportunities and Pitfalls

Agenda

5. Gathering Relevant Information For Disclosure

autm

51

Gathering Information

- Define where in the stack or off-ramp the invention is located and market seeking to cover
  - Does the invention change the blockchain or merely interact with it?
- Define the computer problem and computer solution being offered?
- Identify which blockchain invention was developed for and how it must be modified to work with other blockchain technology
- Understand the details of implementation and why blockchain technology is needed to make the invention work
- Get pseudo code for key aspects of invention
- Identify who is potential infringer and focus on role in performing the claim
- As always, understand why the invention differs from prior art

AMSTER ROTHSTEIN & EBENSTEIN LLP Intellectual Property Law autm 52

AMSTER ROTHSTEIN & EBENSTEIN LLP
Intellectual Property Law

Questions ?????

IP Opportunities and Pitfalls in Protecting Blockchain Technology

Charles R. Macedo, Esq.
cmacedo@arelaw.com

Isabella Ortiz, Esq.
isabella.ortiz@northwestern.edu

A webinar presentation specially prepared for The Association of University Technology Managers (AUTM) Foundation

53

Definitions

Blocks= packages of data that carry permanently recorded data on the blockchain network that contains a timestamp.

Cryptocurrency= digital assets, also known as tokens that are secured against counterfeit and often are not issued or controlled by any centralized authority.

Cryptography=mathematics created codes and ciphers, in order to conceal information. Used to secure and verify transactions on the blockchain (ex. Bitcoin and Ethereum)

Cryptogram= type of puzzle that consists of a short piece of encrypted text.

Decentralized= does not rely on a central point of control.

Distributed Ledger= ledgers in which data is stored across a network of decentralized nodes. It does not have to have its own currency and may be permissioned and private to control who can view it.

ICO= "initial coin offering" a fundraising tool that trades future crypto coins in exchange for cryptocurrencies or immediate, liquid value. Most ICOs work by having investors send funds (i.e. bitcoin) to a smart contract that stores the funds and distributes an equivalent value in the new token at a later point in time. Similar to a IPO in the non-crypto world however startups issues their token in exchange for ether or bitcoin instead of share in a company.

Data Mining= process of adding transaction records to public ledger of past transactions for validating transactions.

Node= copy of the ledger operated by a participant of a blockchain network.

Peer to peer= "P2P" decentralized interactions between two parties or more in highly interconnected network that deal with each other in single mediation point.

54