Patenting Blockchain Technology

Charles R. Macedo, MS
cmacedo@arelaw.com

Jamisue Plucinski
TQAS, Tech Center 3600

Patrick McAtee
SPE, Art Unit 3685

Amster Rothstein & Ebenstein LLP
Intellectual Property Law

UNITED STATES PATENT AND TRADEMARK OFFICE
uspto

Disclaimer

The following presentation reflects the personal opinion of its authors and does not necessarily represent the views of their respective clients, partners, employers or of Amster, Rothstein & Ebenstein LLP, nor the U.S.P.T.O.

Additionally, the following content is presented solely for the purposes of discussion and illustration, and does not comprise, nor is to be considered as, legal advice.

Agenda

Patenting Blockchain Technology

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 It Patent Eligible
5. Avoiding Divided Infringement
6. Identifying the Prior Art

Agenda

Patenting Blockchain Technology

1. Understanding What is Blockchain Technology

Problems vs. Solutions of the Bitcoin Version of Blockchain

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

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

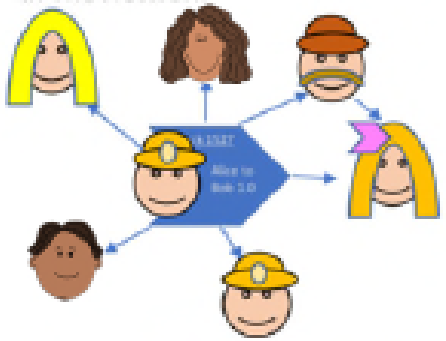
How the Bitcoin Blockchain Works

How Bitcoin Works

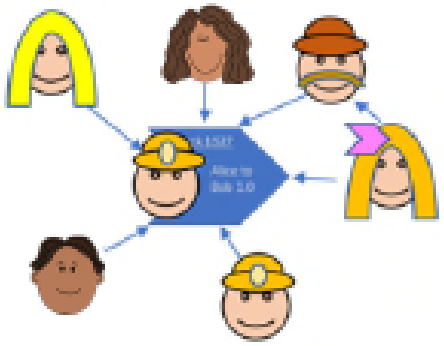
1. Alice sends to Bob 1.00 Bitcoin

2. A Miner Solves A Difficult Math Problem and Saves The Transaction As A Block on the Chain

3. The Block is Broadcast to Everyone In The Network



4. The Block is Approved and Transaction Validated by Network



5. The Block is Added to the Blockchain

6. Bob receives 1 Bitcoin from Alice

Amster Rothstein & Ebenstein LLP
Intellectual Property Law

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)
    a) Other Consensus Mechanisms:
        I. Proof of Stake
        II. Proof of Capacity
        III. Byzantine Fault
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
    1) Alternative – Merkle Tree
6) **Timing of Blocks:** Every 10 minutes

Amster Rothstein & Ebenstein LLP
Intellectual Property Law

“Clones” in Bitcoin Also Inspired Other Bitcoin Like Blockchains

Bitcoin spinoff in 2011 – Quicker block time

namecoin

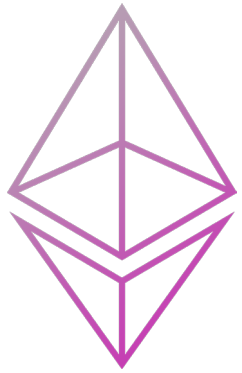
Bitcoin spinoff in 2011 – stores data in transactions

Amster Rothstein & Ebenstein LLP
Intellectual Property Law

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

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

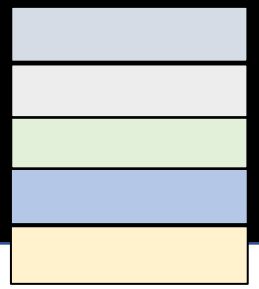
Amster Rothstein & Ebenstein LLP
Intellectual Property Law

Agenda

Patenting Blockchain Technology

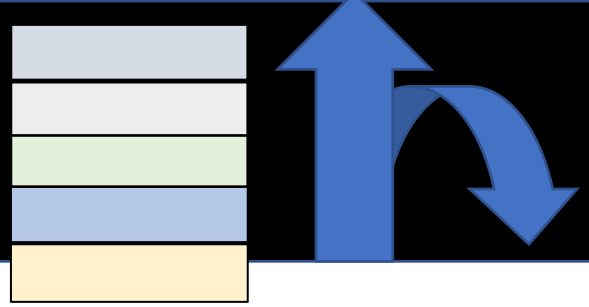
2. Determining What To Patent In The Blockchain Stack

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.
Protocol (Software Code)	e.g., Bitcoin Protocol, Litecoin Protocol, Ethereum Protocol, Zcash Protocol, etc.
Computer Systems Running Protocol	e.g., Nodes (administrator computers), Miners, clients (wallets), custodial systems. etc.

Amster Rothstein & Ebenstein LLP
Intellectual Property Law



Off Ramps

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

Amster Rothstein & Ebenstein LLP
Intellectual Property Law

AMSTER ROTHSTEIN & EBENSTEIN LLP
Intellectual Property Law

Agenda

Patenting Blockchain Technology

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

Patent Evolving Technology

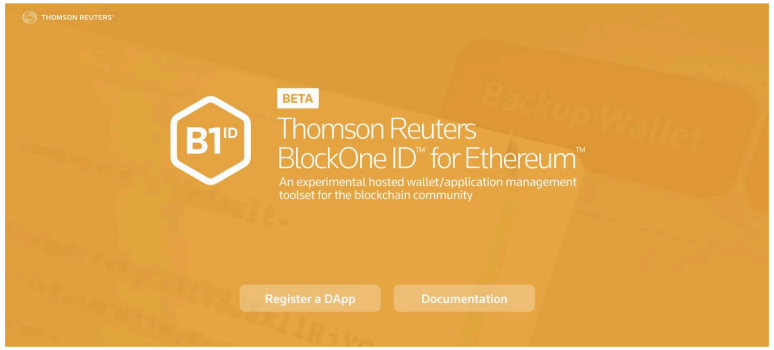
Blockchain Technology is always evolving and disclosure needs to cover variations what might be considered key attributes:

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

Public Blockchains → Private Blockchains

Public Blockchain

Semi-Private Blockchain



Private Blockchain

HYPERLEDGER

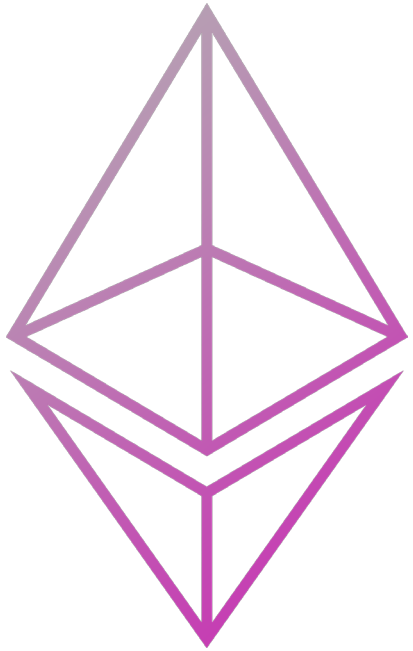
corda

Patent Evolving Technology

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

Proof of Work

Proof of Stake



Byzantine Fault

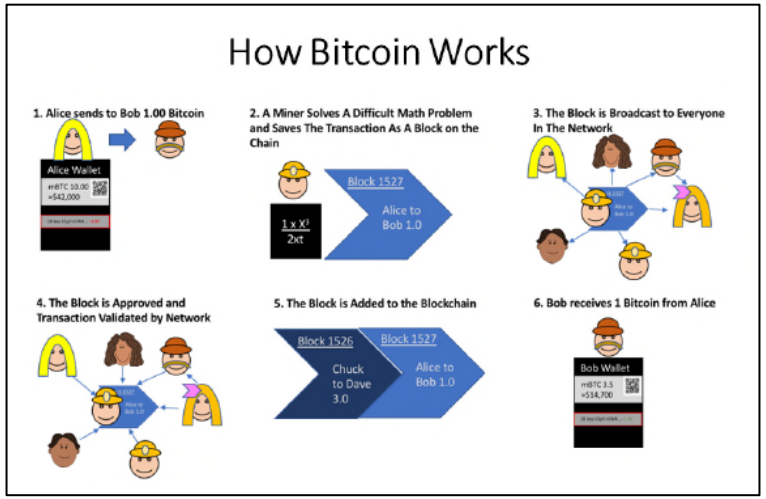
libra

Proof of Capacity

BURST

Sending Messages → Smart contracts and Tokens

Sending Messages



Smart Contracts

PRINT LIMITER Smart Contract
1360

Contract Address 3

PRINT LIMITER Contract Instructions
1360A-1

- PRINT LIMITER Token Creation Instructions Module 1833
- PRINT LIMITER First Authorization Instructions Module 1839
- PRINT LIMITER Second Authorization Instructions Module 1841
- PRINT LIMITER Third Authorization Instructions Module (optional) 1835
- Token Transfer Instructions Module (optional) 1843
- Token Destruction Instructions Module (optional) 1845
- Token Balance Modification Instructions Module (optional) 1847

PROXY Smart Contract
1310

Contract Address 1

PROXY Contract Instructions
1310A-1

- PROXY Delegation Instructions Module 1829
- PROXY Authorization Instructions Module 1831

CUSTODIAN 2 Smart Contract
1350

Contract Address 6

CUSTODIAN 2 Contract Instructions
1350A-1

- CUSTODIAN 2 First Authorization Instructions Module 1849
- CUSTODIAN 2 Second Authorization Instructions Module 1851

Tokens

GEMINI dollar

Public and Transparent Data → Shielded Wallets

Public and Transparent Data

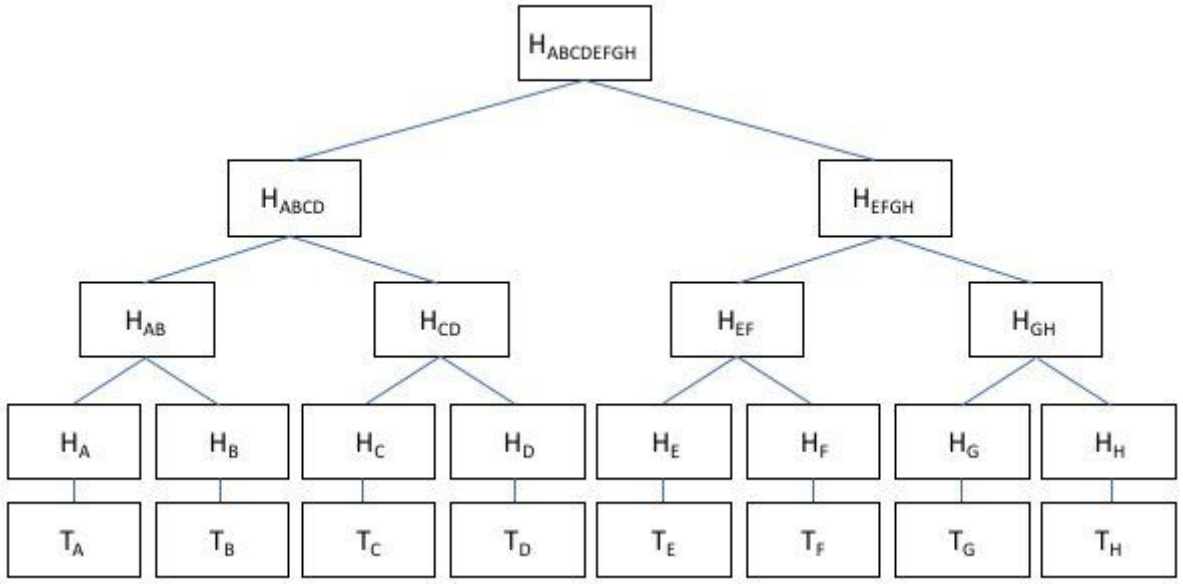
Shielded Wallets

Blockchains and Merkle Trees

Blockchain

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

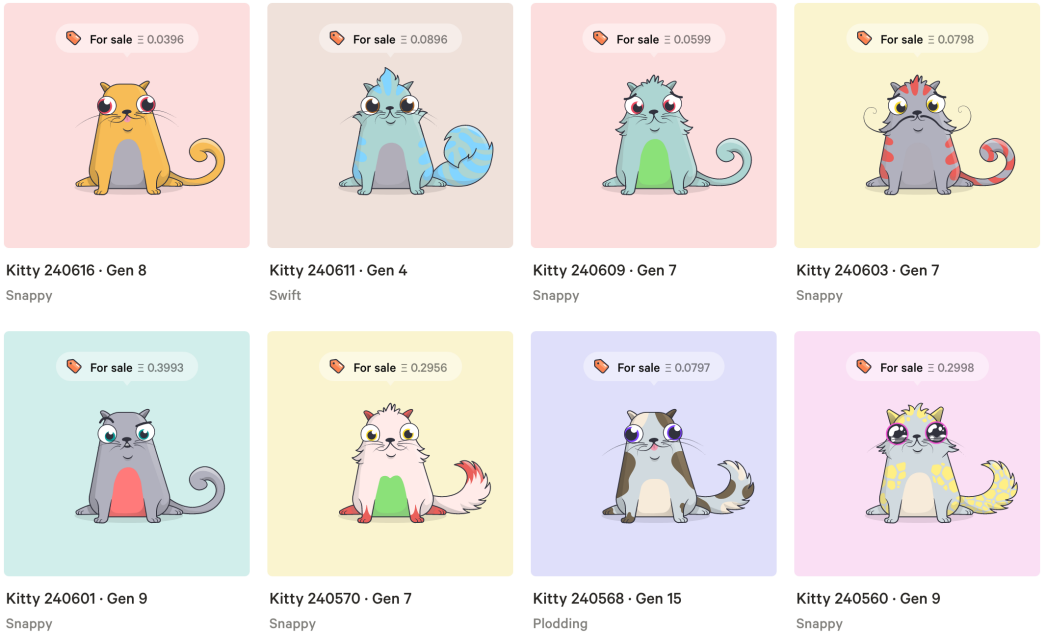
Merkle Tree



Fungible Coins → Nonfungible tokens

Fungible Coins

Non-Fungible Tokens



Agenda

Patenting Blockchain Technology

4. Making It Patent Eligible

Making it Patent Eligible

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

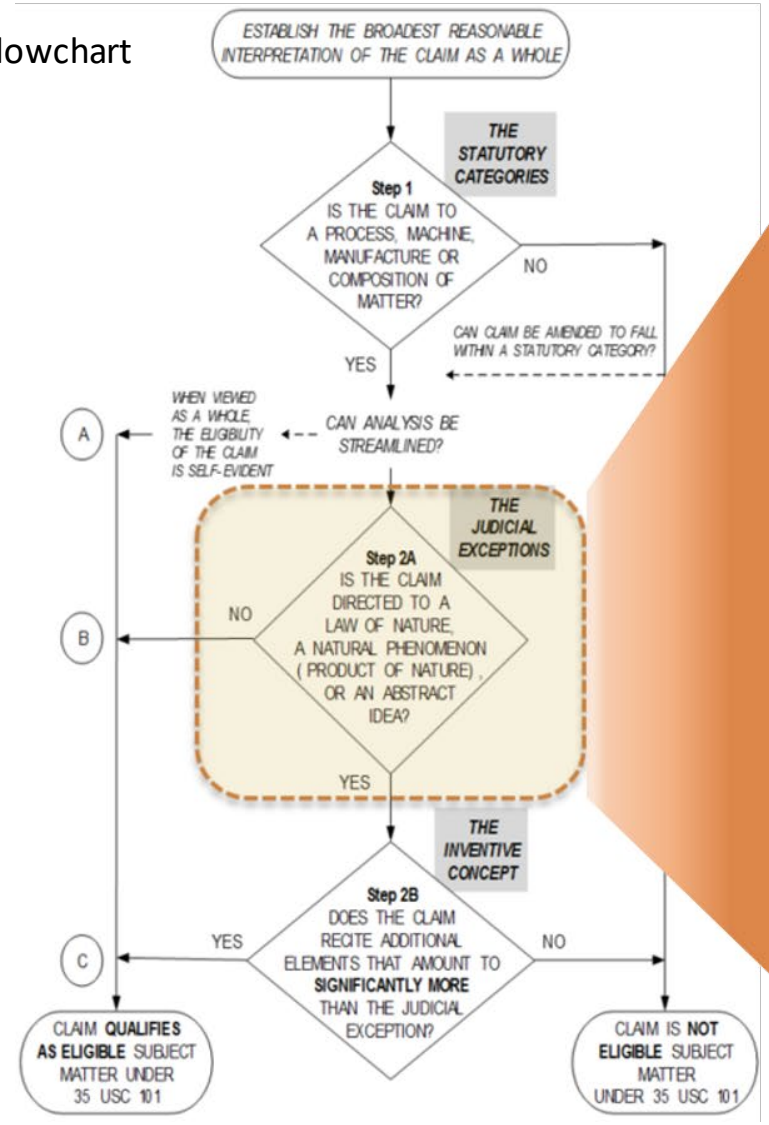
Claims

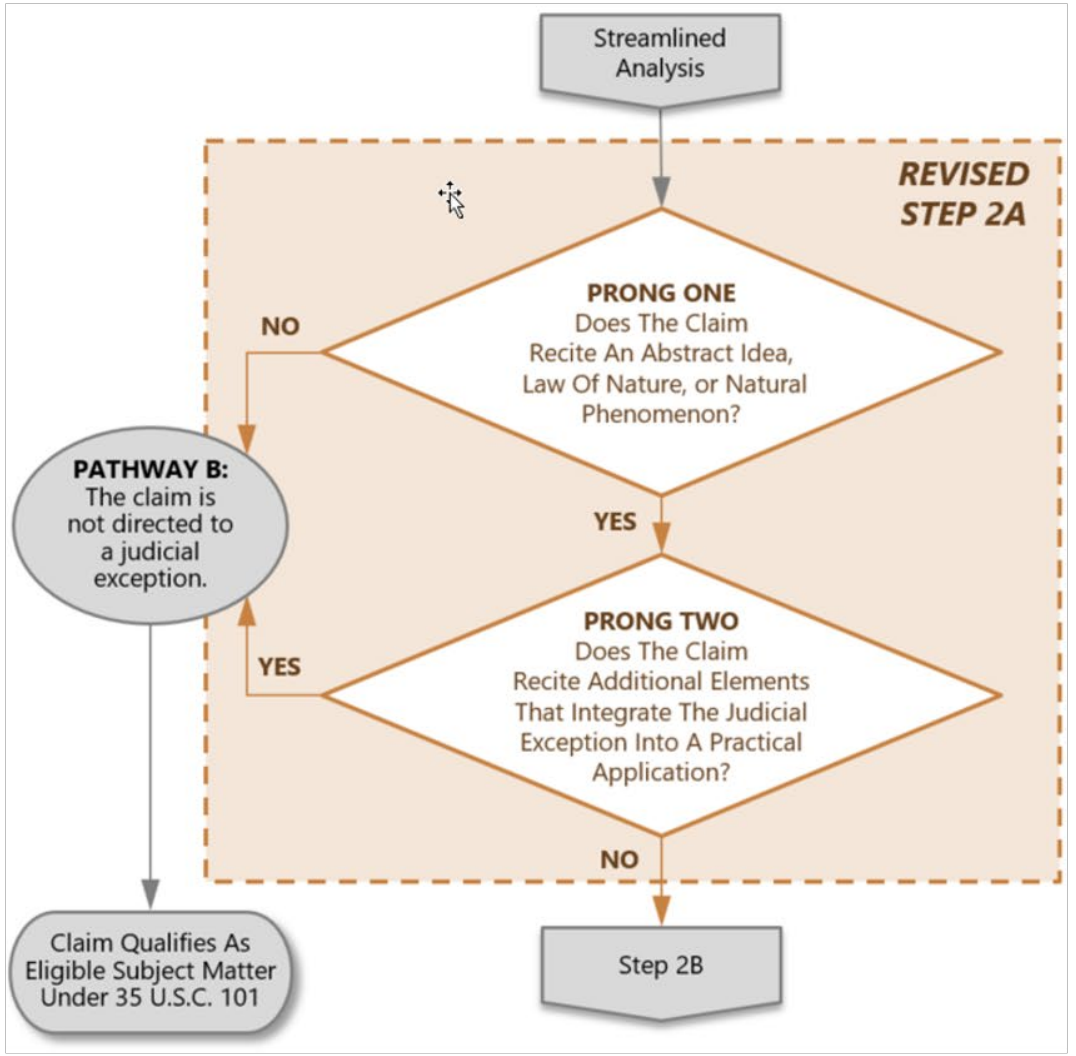
Claims (and specification) should:

- 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

Making it Patent Eligible

MPEP flowchart





Agenda

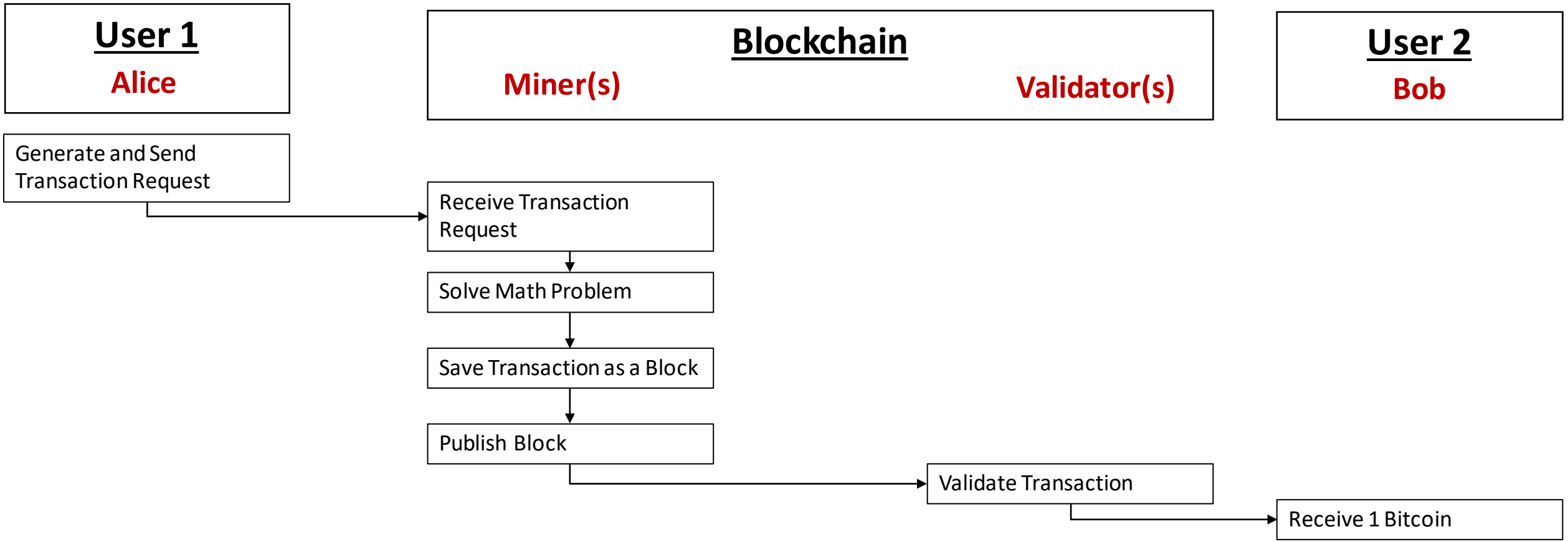
Patenting Blockchain Technology

5. Avoiding Divided Infringement

Avoiding Divided Infringement

- Blockchain technology is based on peer-to-peer networks in which many actors are involved.
- Inventions should be claimed from the perspective of the potential infringer
  - General Exemplary Perspectives:
    - User's Perspective
    - Digital Asset Exchange's Perspective
    - Cryptocurrency Wallet Provider's Perspective
  - Smart Contract Exemplary Perspectives:
    - Issuer's Perspective (e.g. the party who writes the smart contract language)
    - User's Perspective (e.g. the party who interacts with the smart contract)
- Avoid requiring each node to be an active participant to infringe

Exemplary Transaction – Alice Sends Bob 1 Bitcoin



Agenda

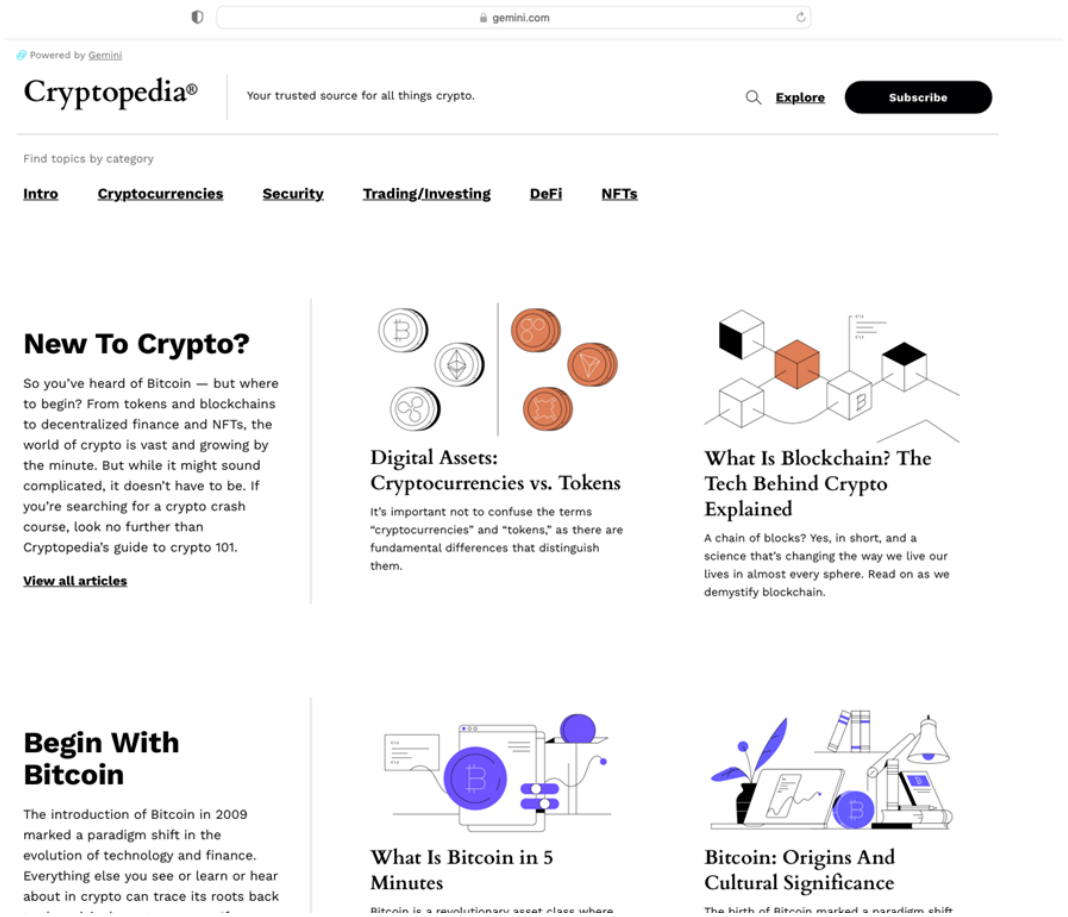
Patenting Blockchain Technology

6. Identifying the Prior Art

Prior Art

Sources of prior art go well beyond traditional patent literature

- News media write about new projects all the time
  - Coindesk.com
  - Medium.com
- White Papers (like the original Satoshi Nakamora 2008 Bitcoin papers) are common
  - https://cbr.stanford.edu/research.html
- GitHub contains lots of repository of relevant code
  - https://github.com/
- Reddit and Quora contain extensive discussions on latest blockchain developments
  - https://www.reddit.com/
  - Quora.com



Patenting Blockchain Technology

Questions ?

Charles R. Macedo, MS
cmacedo@arelaw.com

Jamisue Plucinski
TQAS, Tech Center 3600

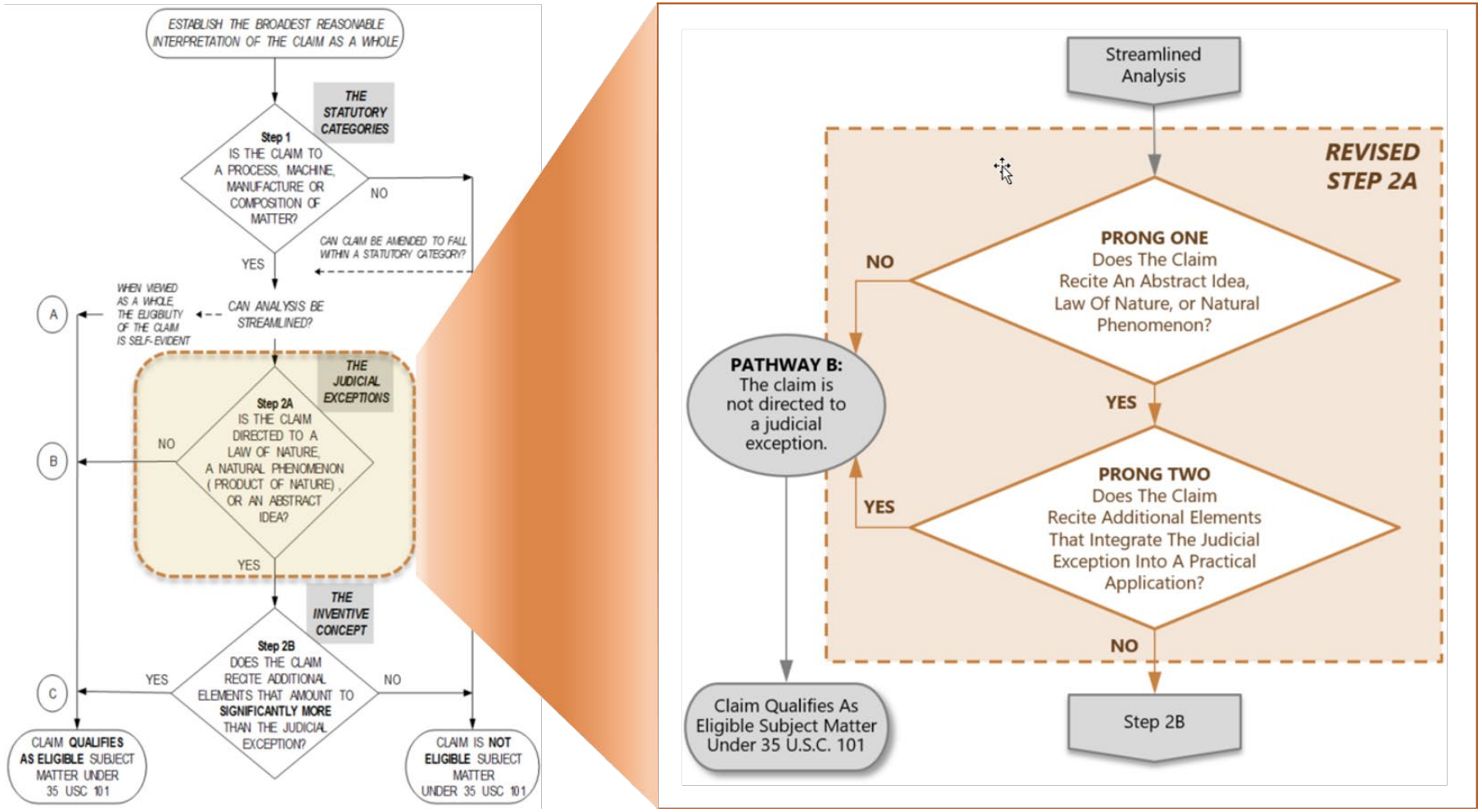
Patrick McAtee
SPE, Art Unit 3685

Amster Rothstein & Ebenstein LLP
Intellectual Property Law

UNITED STATES PATENT AND TRADEMARK OFFICE
uspto

UNITED STATES
PATENT AND TRADEMARK OFFICE

MPEP 2106 flowchart



Groupings of abstract ideas

Mathematical concepts

- Mathematical relationships
- Mathematical formulas or equations
- Mathematical calculations

Mental processes

- Concepts performed in the human mind (including an observation, evaluation, judgment, opinion)

NOTE: The recitation of generic computer components in a claim does not necessarily preclude that claim from reciting an abstract idea.

Certain methods of organizing human activity

- Fundamental economic principles or practices (including hedging, insurance, mitigating risk)
- Commercial or legal interactions (including agreements in the form of contracts; legal obligations; advertising, marketing or sales activities or behaviors; business relations)
- Managing personal behavior or relationships or interactions between people (including social activities, teaching, and following rules or instructions)

Step 2A: Prong two considerations

Limitations that are indicative of integration into a practical application:

- Improvements to the functioning of a computer, or to any other technology or technical field - see MPEP 2106.05(a);
- Applying or using a judicial exception to effect a particular treatment or prophylaxis for a disease or medical condition – see *Vanda* Memo;
- Applying the judicial exception with, or by use of, a particular machine - see MPEP 2106.05(b);
- Effecting a transformation or reduction of a particular article to a different state or thing - see MPEP 2106.05(c); and
- Applying or using the judicial exception in some other meaningful way beyond generally linking the use of the judicial exception to a particular technological environment, such that the claim as a whole is more than a drafting effort designed to monopolize the exception - see MPEP 2106.05(e) and *Vanda* Memo.

Limitations that are **not** indicative of integration into a practical application:

- Adding the words "apply it" (or an equivalent) with the judicial exception, or mere instructions to implement an abstract idea on a computer, or merely uses a computer as a tool to perform an abstract idea - see MPEP 2106.05(f);
- Adding insignificant extra-solution activity to the judicial exception - see MPEP 2106.05(g); and
- Generally linking the use of the judicial exception to a particular technological environment or field of use – see MPEP 2106.05(h)

Whether claim elements represent only well-understood, routine, conventional activity is considered at Step 2B and is not a consideration at Step 2A.

Step 2B considerations

Limitations that are indicative of an inventive concept (aka "significantly more"):

- Improvements to the functioning of a computer, or to any other technology or technical field – see MPEP 2106.05(a);
- Applying the judicial exception with, or by use of, a particular machine – see MPEP 2106.05(b);
- Effecting a transformation or reduction of a particular article to a different state or thing – see MPEP 2106.05(c);
- Applying or using the judicial exception in some other meaningful way beyond generally linking the use of the judicial exception to a particular technological environment, such that the claim as a whole is more than a drafting effort designed to monopolize the exception – see MPEP 2106.05(e) and *Vanda* Memo; and
- **Adding a specific limitation other than what is well-understood, routine, conventional activity in the field – see MPEP 2106.05(d).**

Limitations that are **not** indicative of an inventive concept (aka "significantly more"):

- Adding the words "apply it" (or an equivalent) with the judicial exception, or mere instructions to implement an abstract idea on a computer, or merely uses a computer as a tool to perform an abstract idea – see MPEP 2106.05(f);
- Adding insignificant extra-solution activity to the judicial exception – see MPEP 2106.05(g);
- Generally linking the use of the judicial exception to a particular technological environment or field of use – see MPEP 2106.05(h); and
- **Simply appending well-understood, routine, conventional activities previously known to the industry, specified at a high level of generality, to the judicial exception – see MPEP 2106.05(d) and *Berkheimer* Memo.**

Search and prior art

- MPEP 904: How to Search
  - Analysis of Claims (904.01)
  - General Search Guidelines (904.02)
  - Conducting the Search (904.03)
- MPEP 719.05: Field of Search
  - Searches listed in the “SEARCHED” boxes and/or “SEARCH NOTES” box of the “Search Notes” form

Search and prior art, cont.

- Classification of blockchain-related patent applications

Subject matter	CPC
data structures for information retrieval	G06F 16
protecting data against unauthorized activity	G06F 21
financial, business, cost/price, or management	G06Q
cryptography	H04L 9

- Classification depends on many factors so this is not an exhaustive list


UNITED STATES PATENT AND TRADEMARK OFFICE
DEPARTMENT OF COMMERCE