

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

COINBASE, INC.,

Petitioner

v.

REGINALD MIDDLETON¹

Patent Owner.

IPR 2023-00751

U.S. Patent 11,196,566

**PETITION FOR *INTER PARTES* REVIEW OF
U.S. PATENT 11,196,566**

Mail Stop PATENT BOARD
Patent Trial and Appeal Board
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

¹ Mr. Middleton is the record owner of the '566 patent. According to the Complaint filed in *Veritaseum Capital, LLC v. Coinbase Global, Inc.*, Civ. No. 1:22-cv-01253 (D. Del.), “Mr. Middleton has exclusively licensed all substantial rights to his patents, including the right to sue third parties for infringement of his patents, to Veritaseum Capital, LLC.” (CB-1020, ¶6.)

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. GROUNDS FOR STANDING.....	2
III. IDENTIFICATION OF CHALLENGE	2
A. Prior Art.....	2
B. Grounds for Challenge	3
IV. BACKGROUND	3
A. Technical Background.....	4
1. Decentralized Digital Currencies	4
a. Transactions	5
b. Blockchain	7
2. Cryptography	7
B. The '566 Patent	8
1. Overview	8
a. Swap Embodiment.....	9
b. Network Environment	10
2. The challenged claims are not entitled to benefit of the '566-Prov.....	11
C. Claim Construction	14
D. Level of Ordinary Skill in the Art.....	14
V. GROUND 1: COMBINATION OF HEARN AND ARMSTRONG RENDERS CLAIMS 1-3 OBVIOUS.	15
A. Overview of the Combination	15
1. Hearn	15
2. Armstrong	21
3. Combination of Hearn and Armstrong	25

B.	Claim 1	29
1.	Preamble.....	29
2.	“Memory” [1A].	33
3.	“Network interface” [1B].	36
4.	“Term” [1B.1]-[1B.3].	38
a.	“Principal Data” [1B.1].	39
b.	“Reference” to a “Data Source” [1B.2].	42
c.	“Expiration Timestamp” [1B.3].	43
5.	“Computer Processor” [1C].	45
6.	“Computer Processor” actions [1C.1]-[1C.4].	46
a.	“Read the First Private Key” [1C.1] and “Compute a First Cryptographic Signature” [1C.2].	47
b.	“Create an Inchoate Data Record” [1C.3].	48
(i)	“Commit Input” [1C.3a].	49
(ii)	“One or More Output Data” [1C.3b].	51
(iii)	“First Cryptographic Signature” [1C.3c]	52
c.	“Publish the Inchoate Data Record” [1C.4].	52
7.	“Distributed Ledger” [1D].	53
8.	“Create a Complete Data Record” [1E].	54
9.	“Sign[]” and “Save a Copy of the Inchoate Data Record” [1F].	56
10.	“Verif[y] the Recording of the Complete Data Record in the Distributed Ledger” [1G].	57
C.	Dependent Claim 2	59

D.	Dependent Claim 3	60
VI.	GROUND 2: COMBINATION OF HEARN, ARMSTRONG, AND ZIEGLER RENDERS CLAIMS 7-8 OBVIOUS.	64
A.	Overview of the Combination	64
1.	Ziegler	64
2.	Combination of Hearn, Armstrong, and Ziegler.....	66
B.	Independent Claim 7	67
1.	Preamble [7P].....	68
2.	“ <i>Computing Device</i> ” [7A].....	68
3.	“ <i>First Client Device</i> ” [7B].....	69
a.	“ <i>Memory</i> ” [7B.1], “ <i>Network Interface</i> ” [7B.2], and “ <i>Computer Processor</i> ” [7B.3].....	69
b.	“ <i>Second Computer Processor</i> ” actions.	71
(i)	“ <i>Read the Second Private Key</i> ” [7B.3a], “ <i>Read the Inchoate Data Record</i> ” [7B.3b], “ <i>Compute a Second Cryptographic Signature</i> ” [7B.3c].	72
(ii)	“ <i>Create a Complete Data Record</i> ” [7B.3d].....	73
(iii)	“ <i>Create a Transaction</i> ” [7B.3e].	75
4.	“ <i>Second Client Device</i> ” limitations [7C].	76
5.	“ <i>Sign[]</i> ” and “ <i>Save a Copy of the Inchoate Data Record</i> ” [7D].....	77
6.	“ <i>Distributed Ledger</i> ” [7E].	77
7.	“ <i>Transaction is Created by Broadcasting</i> ” [7F].....	78
8.	“ <i>Verif[y] the Recording of the Complete Data Record in the Distributed Ledger</i> ” [7G].	78
C.	Dependent Claim 8	79

VII.	DISCRETIONARY DENIAL IS NOT APPROPRIATE.	79
A.	35 U.S.C. §325(d).....	79
B.	35 U.S.C. §314(a).....	80
VIII.	MANDATORY NOTICES	80
A.	Real Parties-in-Interest	80
B.	Related Matters.....	80
C.	Lead and Back-Up Counsel.....	81
IX.	CONCLUSION.....	81

EXHIBIT LIST

CB-1001	U.S. Patent 11,196,566 to Middleton (“Middleton”)
CB-1002	File History of U.S. Patent 11,196,566 (“’566 FH”)
CB-1003	Declaration of Dr. Andrew Miller in Support of Petition for <i>Inter Partes</i> Review
CB-1004	Curriculum Vitae of Dr. Andrew Miller
CB-1005	U.S. Provisional Application 61/990,795 (“’566-Prov”)
CB-1006	U.S. Patent Publication 2015/0262168 to Armstrong (“Armstrong”)
CB-1007	U.S. Provisional Application 61/954,434 (“Armstrong-Prov1”)
CB-1008	U.S. Provisional Application 61/990,017 (“Armstrong-Prov2”)
CB-1009	Hearn, “Contracts”, available at https://web.archive.org/web/20140209124419/https://en.bitcoin.it/wiki/Contracts (“Hearn”)
CB-1010	U.S. Patent 7,387,240 to Ziegler (“Ziegler”)
CB-1011	Affidavit of Nathaniel E. Frank-White
CB-1012	Antonopoulos, “Mastering Bitcoin”, chapters 1-4, published on GitHub May 3, 2014 (“Antonopoulos”)
CB-1013	Excerpts from Schneier, “Applied Cryptography”, John Wiley & Sons, Inc. (1996)
CB-1014	Excerpts from Menezes, et al, “Handbook of Applied Cryptography” (1996)
CB-1015	U.S. Patent Publication 2015/0220892 to Allen (“Allen”)
CB-1016	U.S. Patent 8,135,650 to Walker, et al (“Walker”)
CB-1017	Webster’s Encyclopedic Unabridged Dictionary of the English Language, Random House (2001), page 966.
CB-1018	Hearn, “Contract”, available at https://web.archive.org/web/2015110604270/https://en.bitcoin.it/wiki/Contracts

CB-1019	Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System” (2008)
CB-1020	Complaint filed in <i>Veritaseum Capital, LLC v. Coinbase Global, Inc.</i> , Civ. No. 1:22-cv-01253 (D. Del.)
CB-1021	United States District Court - National Judicial Caseload Profile

I. INTRODUCTION

Coinbase, Inc. (“Petitioner”) petitions for *inter partes* review (“IPR”) of claims 1-3, 7, and 8 of U.S. Patent 11,196,566 (“the ’566 patent,” CB-1001). The ’566 patent is directed to a system for “processing a transaction” between parties using a decentralized digital currency such as Bitcoin. The challenged claims recite specific concepts known and used in the existing Bitcoin protocol including cryptographically signed transactions. The ’566 patent admits Bitcoin and other decentralized digital currencies existed and were in use before the ’566 patent.

It is unsurprising then that every aspect of the challenged claims is disclosed in the prior art. Both Hearn and Armstrong use Bitcoin, a well-known cryptocurrency characterized by decentralized computing over a network of computers, specific cryptographic methods, and a common protocol (Bitcoin) to perform blockchain transactions. (See Hearn, CB-1009, 1; Armstrong, CB-1006, ¶3.) Although Hearn does not itself disclose a specific network architecture for using the Bitcoin protocol and transactions to form its contracts, Armstrong discloses an exemplar network architecture for the same Bitcoin transactions Hearn teaches to form its contracts. (CB-1006, ¶3; CB-1009, 5.) Together, these references teach implementation of distributed contracts using exemplar Bitcoin network architecture. The claims are therefore unpatentable.

II. GROUNDS FOR STANDING

Petitioner certifies the '566 patent is available for IPR and Petitioner is not barred or estopped from requesting IPR challenging claims on the grounds identified herein.

III. IDENTIFICATION OF CHALLENGE

A. Prior Art

The '566 patent is the national stage of a PCT application filed May 5, 2015, and claims priority to Provisional Application 61/990,795 (“the '566-Prov”; CB-1005), filed May 9, 2014. Petitioner establishes the '566 patent is not entitled to priority of the '566-Prov in §IV.B.2. The Petition cites the following references, each of which is prior art regardless of the priority date afforded to the '566 patent:

1. **U.S. Patent Publication 2015/0262168 to Armstrong** (“Armstrong”; CB-1006), filed on March 17, 2015, and claiming priority to provisional applications including Application 61/954,434 (“Armstrong-Prov1”; CB-1007) filed March 17, 2014, and Application 61/990,017 (“Armstrong-Prov2”) filed May 7, 2014, is prior art under 35 U.S.C. §102(a)(2). First, Armstrong is entitled to benefit of both Armstrong-Prov1 and Armstrong-Prov2 as Petitioner demonstrates throughout §V and is therefore prior art as of the provisional applications’ filing dates. Second, even if Armstrong is not entitled to benefit of Armstrong-Prov1 or

Armstrong-Prov2, Armstrong was filed before May 5, 2015, the earliest priority date of the '566 patent. *See* §IV.B.2.

2. **“Contracts” to Hearn** (“Hearn”; CB-1009) is prior art under 35 U.S.C. §102(a)(2) because it was publicly available via the website, <https://en.bitcoin.it/wiki/Contracts>, prior to May 5, 2015. (*See* CB-1011, 1-3, 19-25 (documenting availability by May 9, 2014).) The '566 patent confirms Hearn was published by April 9, 2014, citing Hearn in multiple places as admitted prior art. (*See* CB-1001, 3:53-55, 3:61-62.)

3. **U.S. Patent 7,387,240 to Ziegler** (“Zeigler”; CB-1010), issued June 17, 2008, is prior art under 35 U.S.C. §102(a)(2).

Neither Armstrong, Hearn, or Ziegler were applied or discussed on the record during prosecution of the '566 patent. (*See* CB-1002.)

B. Grounds for Challenge

Ground 1: Combination of Hearn and Armstrong renders claims 1-3 obvious.

Ground 2: Combination of Hearn, Armstrong, and Ziegler renders claims 7-8 obvious.

IV. BACKGROUND

The '566 patent “pertains to systems and methods enabling parties with little trust or no trust in each other to enter into and enforce agreements ...without

special technical knowledge of the underlying transfer mechanism(s)” (e.g., decentralized digital currency. (CB-1001, 5:48-53; *see also*, 38:8-11 (defining “transfer mechanism”).) The ’566 patent therefore does nothing more than document well-known concepts in existing decentralized digital currencies such as Bitcoin.

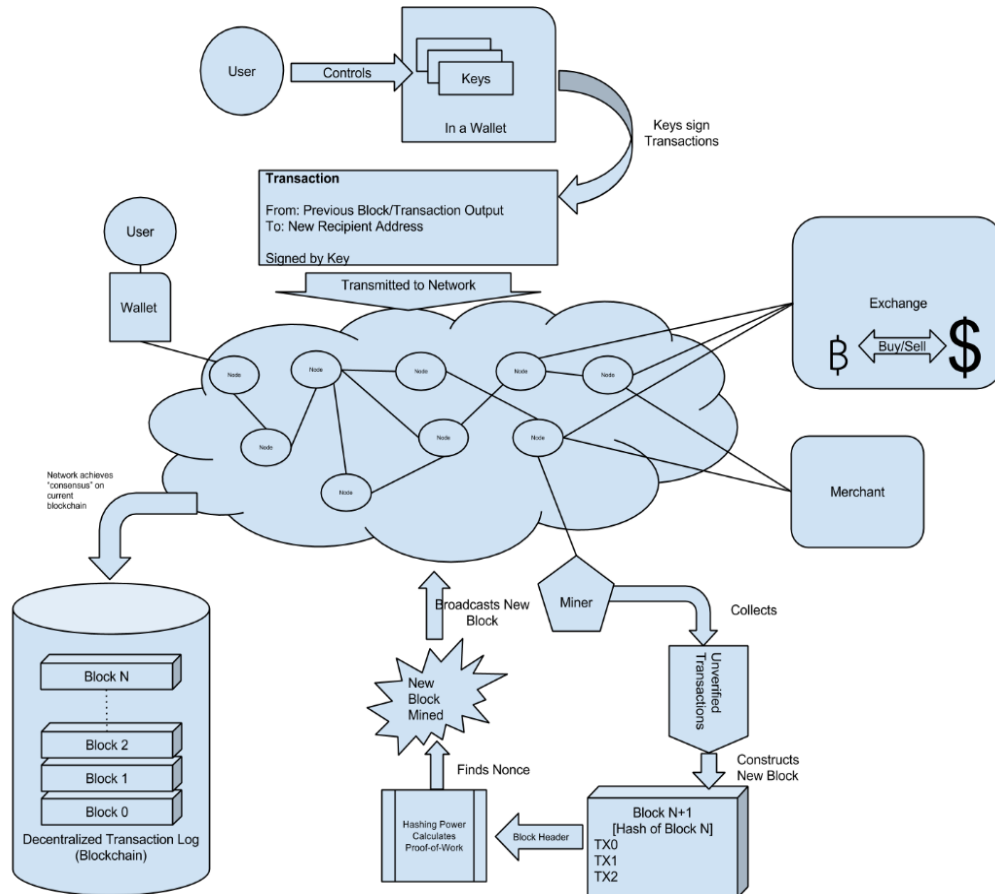
A. Technical Background

1. Decentralized Digital Currencies

The ’566 patent provides a lengthy section detailing admitted prior art, including existing decentralized digital currencies. The ’566 patent acknowledges “decentralized digital currencies generally operate by maintaining a whole or partial history of ‘ledger’ (sometimes referred to as a ‘block chain’) of all transactions that have been ‘validated’ by a consensus of network participants.” (CB-1001, 2:44-49.) One such existing decentralized currency was Bitcoin. (*See* CB-1001, 2:40-43 (“The Bitcoin protocol and progeny ... are one such class of technologies that have recently enjoyed meteoric rises in popularity (and valuation)”); CB-1019.)

“Bitcoin is a fully-distributed, peer-to-peer system.” (CB-1012, 1.) Currency units called “bitcoins are used to store and transmit value among participants in the bitcoin network.” (CB-1012, 1.) Coins are “stored on the blockchain in the form of transaction-outputs.” (CB-1012, 40.) The following figure, from Antonopoulos

illustrates an illustrative Bitcoin system, consisting “of users with wallets containing keys, transactions which are propagated across the network and miners who produce (through competitive computation) the consensus blockchain, the authoritative ledger of transactions.” (CB-1012, 9.)



Antonopoulos, Chapter 2

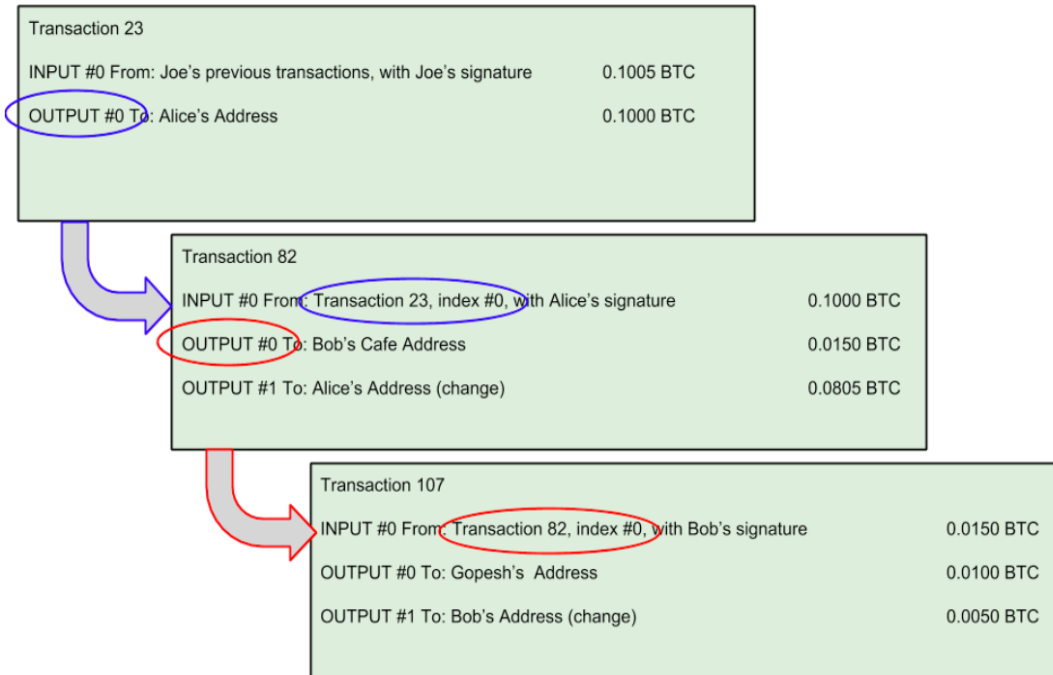
a. Transactions

Transactions are an important part of the Bitcoin system. A “transaction tells the network that the owner of a number of bitcoins has authorized the transfer of some of these bitcoins to another owner.” (CB-1012, 11.) The new owner

“spend[s] these bitcoins by creating another transaction that authorizes transfer to another owner, and so on, in a chain of ownership.” (*Id.*)

A “transaction comprises at least one input and at least one output.” (CB-1001, 2:51-52.) An input “is where the coin value is coming from, usually a previous transaction’s output.” (CB-1012, 12.) The transaction output “assigns a new owner to the value by associating it with a key.” (*Id.*) The key “imposes a requirement for a signature” to redeem the funds in future transactions. (*Id.*) If an output can be claimed by providing a single signature, it is referred to as a “singlesig” output. (CB-1003, ¶29.) In contrast, a multiple signature or “multisig” output specifies a set of *n* keys and requires *m*-of-*n* valid signatures from keys in the set to be valid. (*Id.*) For example, in a 2-of-2 output, two parties (e.g., A and B) must sign transactions spending the output. (*Id.*)

A transaction output is considered “spent” if it is associated with a valid child transaction and “unspent” if it is not associated with a valid child transaction, as illustrated in the following figure from Antonopoulos. (CB-1001, 2:61-66; CB-1012, 13-14.) “For the transaction to be valid, every input must be an unspent output of a previous transaction.” (CB-1001, 4:45-46.)



Antonopoulos, Chapter 2

b. Blockchain

The blockchain “is a public ledger that records bitcoin transactions.” (CB-1001, 3:63-64.) To be recorded in the blockchain, a transaction is broadcast to the Bitcoin network, “‘picked up’ by a miner and included in a block of transactions.” (CB-1012, 7.) A transaction “is only ‘trusted’ by all when it is included in a newly mined block.” (*Id.*)

2. Cryptography

In cryptocurrencies, cryptographic algorithms ensure parties are authorized to participate in a proposed transaction. (*See* CB-1012, 40-49.) Two types of cryptographic algorithms exist—symmetric and public-key algorithms. (CB-1013, 4-5.) Symmetric algorithms use the same key to encrypt and decrypt data. (CB-

1003, ¶34, *citing* CB-1013, 4.) Asymmetric (or public-key) algorithms use two keys that are mathematically related. (CB-1013, 464.) One key is kept private (the private key) and the other key is distributed publicly (the public key). (CB-1013, 4-5.)

Asymmetric keys are commonly used to create digital signatures which enable a user to sign a transaction proving ownership. (*See* CB-1012, 40.) To create a signature, a party computes a hash of the transaction (referred to as a digest) and encrypts the digest with the party's private key. (CB-1013, 38.) A recipient verifies the signature by decrypting the signature using the party's public key to recover the digest. (*Id.*) The recipient independently computes the digest and compares it to the decrypted version. (*Id.*) If the message has not been altered, the calculated and recovered digests will be the same. (*Id.*)

B. The '566 Patent

1. Overview

The '566 patent describes systems enabling parties to enter into and enforce agreements. (*See, e.g.*, CB-1001, 5:48-55.) The specification provides exemplary embodiments of such agreements including swaps. (CB-1001, 5:60-61.)

a. Swap Embodiment

For example, the '566 patent describes the “major phases effecting a value transfer in the form of a swap.” (CB-1001, 35:27-30.) This embodiment follows substantially the same flow as Hearn’s Example 7. (*See* §V.A.1.)

In a first phase, the client “validates a first order comprising terms (e.g., base instrument, quote instrument, principal, collateral, disbursement function, expiration timestamp, etc.).” (CB-1001, 35:30-34.) The client then “submits (broadcasts) a first principal transaction record conforming to the terms to the transfer mechanism to create a first principal transaction.” (CB-1001, 35:34-37.)

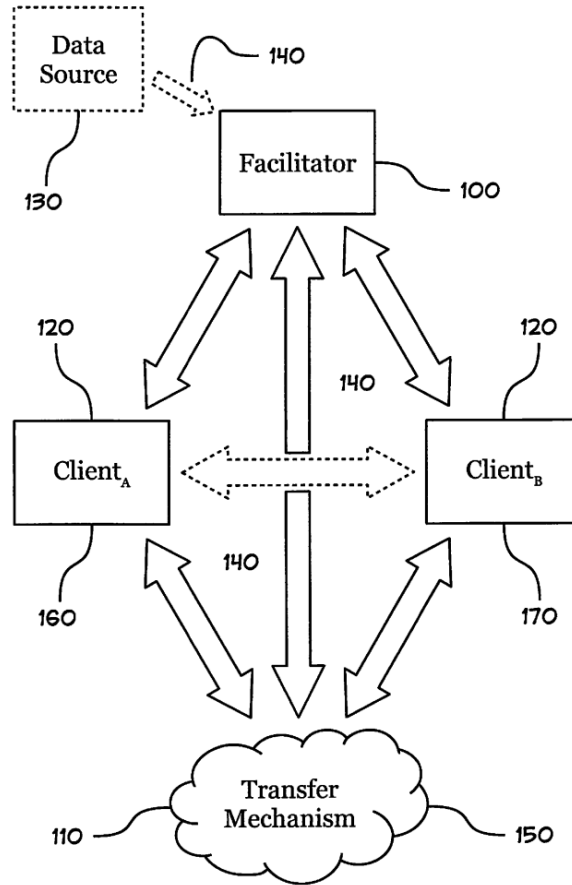
In the second phase, the outputs from the first principal transaction are committed “by creating and submitting (broadcasting) a commit transaction record to the transfer mechanism to create a commit transaction.” (CB-1001, 35:39-45.) Optionally, “a refund or ‘rollback’ transaction record” is created and made available for the client “that spends the outputs from the commit transaction, but cannot be used until well after the expiration timestamp.” (CB-1001, 35:45-48.) In this way, “[i]f the facilitator fails catastrophically,” the client can “sign and submit the refund transaction record to place” the client back in its original position. (CB-1001, 35:48-51.)

In the third phase, a value is received from a data source and the valuation is monitored “by applying a disbursement function to the value[]”, the principal, and

any collateral to check whether the principal and any collateral of any one party is exhausted.” (CB-1001, 35:52-56.) In a final phase, “after the expiration timestamp (or if the principal and any collateral of any party is exhausted, whichever is sooner),” an inchoate disbursement transaction “that spends the commit transaction’s output(s)” is created and signed. (CB-1001, 35:59-66.) When the inchoate disbursement transaction is completed, the “client submits (broadcasts) the complete disbursement transaction record to the transfer mechanism to create the disbursement transaction.” (CB-1001, 35:66-36:4.)

b. Network Environment

The ’566 patent depicts an exemplary network environment for implementing its agreements in Figure 1 (below). The network includes a transfer mechanism (110) such as a decentralized digital currency (150), clients (120, 160, 170), facilitator (100), and data source (130) connected by a computer network (140). (CB-1001, 7:9-14, 8:49-49.)



'566 Patent, Figure 1

2. The challenged claims are not entitled to benefit of the '566-Prov

The challenged claims are not entitled to priority benefit of the '566-Prov because the provisional lacks written description support for the limitation that “*at least one of the computing device, the first client device, or the second client device verifies the recording of the complete data record in the distributed ledger by observing an external state*”² ([1G]/[7G]). To obtain priority benefit to an earlier-

² Limitations of the challenged claims are indicated by italics throughout.

filed application, the earlier-filed application must provide written description support for the claimed invention. 35 U.S.C. § 112(a). To satisfy the written description requirement, the earlier-filed application must “convey with reasonable clarity to those skilled in the art that, as of the filing date sought, [the inventor] was in possession of *the invention*.” *Vas-Cath Inc. v. Mahurkar*, 935 F.2d 1555, 1563-64 (Fed. Cir. 1991) (emphasis in original). The ’566-Prov fails to show possession of limitations [1G]/[7G].

The ’566-Prov does not explicitly disclose verification by any network device of “*the recording of the complete data record in the distributed ledger by observing **an external state***”³ or “**verify[ing]** *the recording of the complete data record in the distributed ledger.*” Moreover, the two brief mentions of “*external state*” in the ’566-Prov are unrelated to verification of the recording of a data record in a distributed ledger. Both examples describe transactions in which assets committed to a transaction are **released** based on observation of an external state such as “the relative value of certain assets at a certain time” or “verification of delivery to a shipper or an address.” (CB-1005, ¶¶17-18.) These have nothing to do with a distributed ledger. (CB-1003, ¶52.)

³ Unless otherwise indicated all emphasis added.

Limitations [1G]/[7G] were added to claims 1 and 7 late in prosecution to overcome §101 rejections. (CB-1002, 505-533, 590-605, 613-632.) When making the amendment, Applicant cited to 12 paragraphs of the published patent application as supporting the amendment.⁴ (CB-1002, 613.) Of these cited paragraphs, 6 were newly added in the publication and the remaining 6 correspond to paragraphs 8 and 43-36 of the '566-Prov. But these paragraphs do not explicitly disclose the subject matter of [1G]/[7G]. Paragraph 8 merely discusses well-known aspects of transaction inputs and outputs used in cryptocurrencies such as Bitcoin. There is no mention in this paragraph of a “*distributed ledger*” or recording of a transaction in a ledger. And paragraphs 43-46 describe a swap embodiment with no mention of recording a transaction in a distributed ledger let alone verification of the recording.

The claimed verification is also not inherently disclosed in the '566-Prov. *See Nuvo Pharms. (Ireland) Designated Activity Co. v. Dr. Reddy's Lab'ys Inc.*, 923 F.3d 1368, 1382-83 (Fed. Cir. 2019) (“[U]nder a narrow set of circumstances, the written description requirement may be satisfied without an explicit disclosure

⁴ Petitioner does not acquiesce limitations [1G] and [7G] are supported by the '566 patent and reserves the right to argue invalidity under 35 U.S.C. §112 in another forum.

if the claimed features are necessarily inherent in what is expressly described.”)

The mere mention of “blockchain” in the provisional and the known aspects of the Bitcoin protocol related to the use of “blockchain” is not sufficient to establish that verification of “*the recording of the complete data record in the distributed ledger by observing **an external state***” is necessarily present in the ’566 patent.

Accordingly, the ’566-Prov does not convey to the POSITA possession of the subject matter of limitations [1G]/[7G] and the challenged claims are not entitled to priority to the ’566-Prov. (CB-1003, ¶¶48-52.)

C. Claim Construction

Petitioner does not believe any claims require construction to resolve the patentability disputes in this proceeding. Accordingly, Petitioner applies the plain and ordinary meaning for each term in the challenged claims.

D. Level of Ordinary Skill in the Art

A person having ordinary skill in the art (“POSITA”) would possess either (i) a Bachelor of Science degree in computer science, computer engineering, electrical engineering, or mathematics, or equivalent and 2-3 years of experience in implementation, programming, or design of cryptocurrencies or blockchain technologies; or (ii) a doctoral degree in computer science, computer engineering, electrical engineering, or mathematics, or equivalent with experience in

cryptography including the study, design, or implementation thereof for use in computer systems. (CB-1003, ¶55.)

**V. GROUND 1: COMBINATION OF HEARN AND ARMSTRONG
RENDERS CLAIMS 1-3 OBVIOUS**

A. Overview of the Combination

1. Hearn

Hearn describes a set of “distributed contract[s]” which “us[e] Bitcoin to form agreements with people via the block chain.” (CB-1009, 1.) Hearn’s distributed contracts allow agreements to be encoded using Bitcoin transactions which guarantee an action agreed upon by a contract’s parties is performed. (CB-1003, ¶56.) The present combination focuses on “Example 7”—“[r]apidly-adjusted (micro)payments to a pre-determined party.” (CB-1009, 5.)

A micropayment is a small payment between parties. (CB-1003, ¶58.) Because of transaction fees, it has not been cost-effective to use existing credit/debit cards for such small payments. (*Id.*) Hearn presents a micropayment protocol allowing a party to accept metered payments from another party over the duration of a service while minimizing transaction costs. (*Id.*) In Hearn’s micropayment example, Party A (client) wishes “to pay 0.001 BTC per 10 kilobytes of usage” of an untrusted café’s Wi-Fi hotspot “without opening an account with the café.” (CB-1009, 5.) Hearn’s micropayment protocol allows Party A (client) to pay the untrusted server (Party B) as it uses the Wi-Fi service. (*Id.*)

Hearn's micropayment protocol works in two stages. In the first stage, a micropayment channel is established between Party A (client) and Party B (server) placing in escrow a maximum expected amount to be paid for the micropayment contract. (*See* CB-1009, 5 (steps 1-2).) In the second stage, Party A makes small usage-based payments which increment the total to be paid to Party B for the service over the duration of the contract. (*See*, CB-1009, 5 (steps 7-9).) Party B only broadcasts the final payment transaction to the Bitcoin network. Through this technique, described further below, only two transactions (the “escrow” and final payment transactions) are broadcast, minimizing the total Bitcoin transactions fees. (CB-1003, ¶59.)

STAGE 1: ESTABLISHING THE CHANNEL

After creation of a public key for Party A and receipt of a public key for Party B (step 1), Party A creates and signs a “transaction (T1) that sets up a payment of (for example) 10 BTC to an output requiring both the server's public key and one of [the client's own keys] to be used” (step 2). (CB-1009, 5.) Hearn discloses that a “good way to do this is use the OP_CHECKMULTISIG” capability. (*Id.*) Transaction T1, illustrated in Miller Figure A⁵ below, acts as an

⁵ “Miller Figure” herein refers to a figure from the Miller Declaration, CB-

“escrow” transaction transferring the maximum anticipated total value to be paid under the contract (e.g., 10 BTC) **from** the output funds of a previous transaction owned by A **to** an “escrow” account owned by both Party A and Party B. (CB-1003, ¶63.) The “escrow” transaction commits funds to the channel. (*Id.*) Any transactions spending the bitcoin of this new “escrow” account must be signed by both Party A and Party B.

Transaction ID (T1)

INPUTS From:

previous transaction received by Party A 10 BTC
with Party A's DIGITAL SIGNATURE

OUTPUTS To:

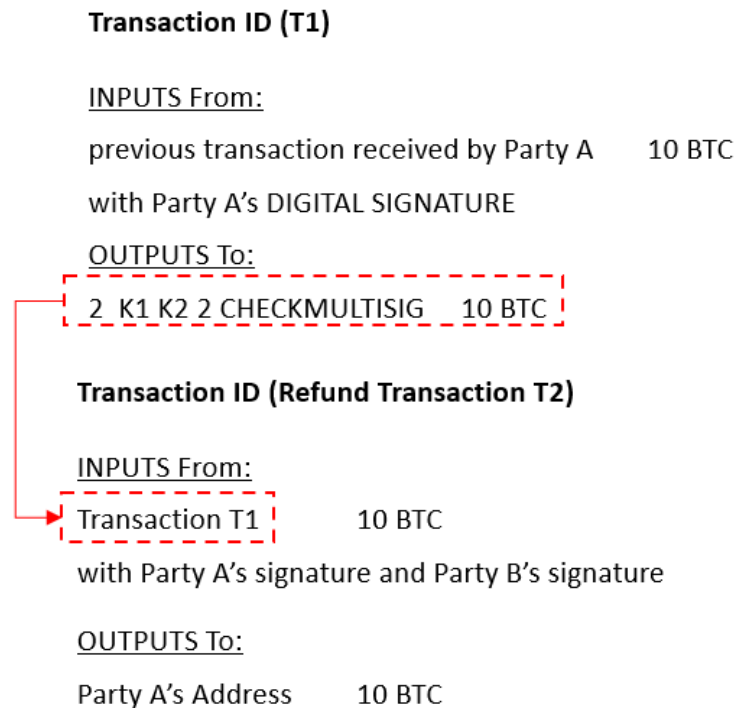
2 K1 K2 2 CHECKMULTISIG 10 BTC

Miller, Figure A

Next, Party A creates a refund transaction (T2), which takes as input the output of the “escrow” transaction T1 and refunds “all the money back” to Party A. (CB-1009, 5 (step 3).) The refund transaction (T2), illustrated in Miller Figure B below, spends the multisig output of T1 and transfers the maximum anticipated total value (e.g., 10 BTC) to an address associated with Party A. (CB-1003, ¶64.)

1003.

The transaction is locked to ensure the transaction cannot be accepted into the blockchain until a specified time window has expired. (CB-1009, 5 (“It has a time lock set for some time in the future, for instance a few hours.”).) That is, Party A cannot redeem the refund until after this lock time has expired. (CB-1003, ¶64.) Refund transaction T2 allows Party A to reclaim its committed bitcoin if Party B becomes unresponsive or uncooperative. (*Id.*; CB-1009, 5 (“The refund transaction is needed to handle the case where the server disappears or halts at any point, leaving the allocated value in limbo”).)



Miller, Figure B

Party A sends the refund transaction (T2) to Party B which signs the refund transaction⁶ (step 4) and returns the signature to Party A. (CB-1009, 5 (steps 3-4).) Party A verifies the signature using Party B's public key (step 5). If the signature is valid, Party A (client) signs the "escrow" transaction T1 and "passes the signature to" Party B (server). (CB-1009, 5 (step 6). The server then "broadcasts the transaction" (T1). (CB-1009, 5 (step 6).) "Broadcasting" transaction T1 commits T1 to the blockchain which "locks in the money." (CB-1003, ¶66; CB-1009, 5.) The broadcasting of T1 also indicates Party A can start making incremental payments to Party B. (CB-1003, ¶66.)

STAGE 2: MAKING PAYMENTS

As Party B provides Wi-Fi access to Party A, Party A issues a series of transactions transferring more and more of the amount in the shared "escrow" account to Party B and less and less to itself. (*See* CB-1009, 5 (step 9).)

⁶ In step 4, Hearn states the "server signs T2 using its public key K2." (CB-1009, 5 (step 4)) A POSITA would have understood this is a typographical error and should be interpreted as the "server signs T2 using its **private** key." (CB-1003, ¶65.) Indeed, later versions of the Contract paper have corrected this error. (CB-1018, 5.)

Specifically, Party A creates an initial payment transaction T3 “which connects to T1 like the refund transaction and has two outputs”—one goes to Party A and the other goes to Party B.⁷ (CB-1009, 5 (step 7).) In this initial payment transaction, all value of T1 is “allocated to the first output (K1).” (*Id.*) Party A “signs T3 and provides the signature” to Party B. (*Id.*)

Party A then provides metered payments to Party B. Specifically, Party A adjusts its copy of T3 to allocate more value to Party B’s output (K2) and less to its own (K1). (*Id.* (step 9).) For example, Party A may send an updated transaction after a pre-determined amount of usage (e.g., 100 kilobytes). (CB-1003, ¶68.) Party A “re-signs the new T3 and sends the signature to the server.” (CB-1009, 5 (step 9).) The server then “adjusts its copy of T3 to match the new amounts, verifies the signature and continues.” (*Id.*) These transactions are not broadcast. Accordingly, the most that can be lost by Party A if the server stops providing Wi-Fi service is one small incremental payment. (CB-1003, ¶68.)

Because all the updated payment transactions T3 spend the same output, only one version can be committed to the blockchain. (CB-1003, ¶69.) Party B therefore broadcasts the final payment update which allocates the maximum

⁷ In step 7, Hearn also refers to the parties by their associated public keys.

K1 refers to Party A and K2 refers to Party B. (CB-1003, ¶67.)

amount of the “escrow” transaction to Party B and effectively closes the payment channel between the parties. (*Id.*) This occurs when the session ends (e.g., both parties agree to close the channel) or a pre-determined time period is close to expiring. (CB-1009, 5 (“This continues until the session ends, or the 1-day period is getting close to expiry. The AP then signs and broadcasts the last transaction it saw, allocating the final amount to itself”).)

2. Armstrong

Armstrong relates to a “system and method for transacting bitcoin” such as the Bitcoin transactions used in Hearn’s Example 7. (CB-1006, ¶3; CB-1007, ¶1; CB-1008, ¶1.) Armstrong is prior art to the ’566 patent as of its non-provisional filing date (March 17, 2015) because the ’566 patent is not entitled to priority to its provisional. (*See* §IV.B.2.)

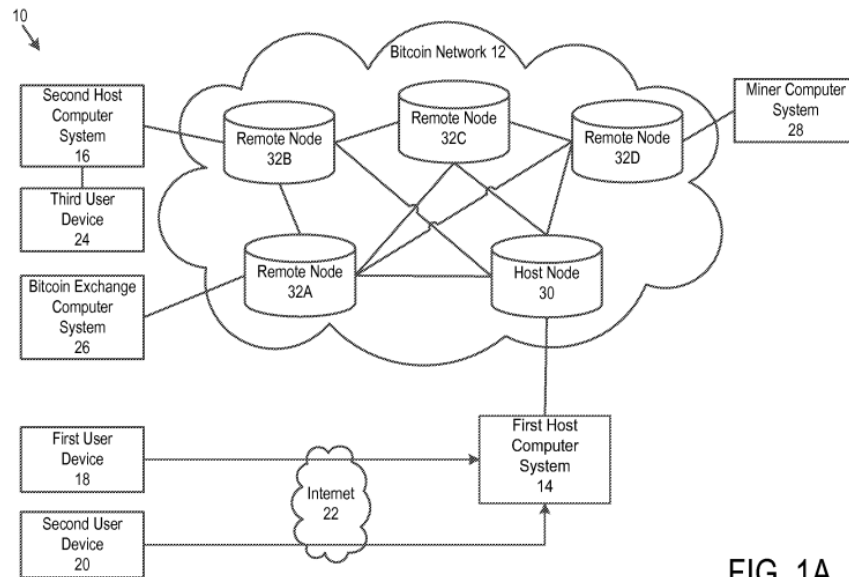
Should PO argue the ’566 patent is entitled to priority of its provisional, Armstrong remains prior art because Armstrong is entitled to priority benefit to at least Armstrong-Prov1, filed March 17, 2014 and Armstrong-Prov2, filed May 7, 2014. Under 35 U.S.C. §102(a)(2), a published patent application is prior art as of its effective filing date. An application is considered to have been effectively filed, with respect to any subject matter described in the application, as of the filing date

of the earliest application describing the subject matter⁸ to which the application is entitled to claim a right of priority. 35 U.S.C. §102(d)(2); *See* IPR2022-00341, *Apple Inc. v. Telefonaktiebolaget LM Ericsson*, Paper 10, 16-22 (PTAB Sept. 14, 2022) (finding *Dynamic Drinkware* does not apply to post-AIA patents)).

Armstrong is entitled to priority benefit of Armstrong-Prov1 and Armstrong-Prov2 under §119(e) because it was filed not later than 12 months after the date on which each provisional was filed and contains a specific reference to each provisional application. (*See* CB-1006, ¶1.) Petitioner provides cross-cites to Armstrong-Prov1 and Armstrong-Prov2 throughout to demonstrate the subject matter relied from Armstrong is disclosed in both provisionals.

Armstrong discloses an exemplary network environment 10 for processing Bitcoin transactions, illustrated in Figure 1A below, including Bitcoin network 12, host computers 14 and 16, and user devices 18 and 20 connected over the Internet 22 to first host computer 14. (CB-1006, ¶81; CB-1007, ¶¶32-33; CB-1008, ¶¶47-48, Figure 1A.)

⁸ Should PO incorrectly contend that *Dynamic Drinkware* framework applies to AIA patents, Petitioner's expert demonstrates that at least one claim of Armstrong is supported by Armstrong-Prov1 and Armstrong-Prov2. (CB-1003, ¶78.)



Armstrong, Figure 1A

First host computer 14 “is used primarily for transacting bitcoin”, as illustrated in Figure 1B. (CB-1006, ¶83; CB-1007, ¶34; CB-1008, ¶49.) A host computer “host[s] accounts or ‘wallets’ that allow users to make and accept payments using bitcoin.” (CB-1006, ¶8; CB-1007, ¶5; CB-1008, ¶5.) Armstrong explains when a transaction is made between two wallets at different host computers, “the transaction is broadcast to the Bitcoin network for block chain verification.” (CB-1006, ¶10; CB-1007, ¶7; CB-1008, ¶7.) A transaction (Transfer 7) between a wallet held by first host computer 14 and a wallet held by second host computer 16 (e.g., Wallet C) is illustrated in Figure 45 below. A user enters a bitcoin address (Bitcoin address 6) “located in the third wallet (Wallet C) and an amount of bitcoin to be transferred to the third wallet (Wallet C).” (CB-1006, ¶103;

CB-1007, ¶54; CB-1008, ¶69.) The transfer (in red box below) “is recorded within the second wallet (Wallet B).” (CB-1006, ¶103; CB-1007, ¶54; CB-1008, ¶69.)

	First Host Computer System 14			Second Host Computer System 16	
	Wallet A		Wallet B	Wallet C	
	Email Address A; Login Details		Email Address B; Login Details		
Transfer 1	Bitcoin address 1				
		Amount in bitcoin			
	Bitcoin address 2				
Transfer 2		From: Network address			
		Amount in bitcoin			
		Host Fee: 0 bitcoin			
Transfer 3	Bitcoin address 2		Bitcoin address 3		
		To: Email address B	From: Wallet A		
		Amount in bitcoin	Amount in bitcoin		
		Miner's Fee = 0 bitcoin			
		Host Fee: 0 bitcoin			
Transfer 4			Bitcoin address 4		
			From: First Host		
			Amount in bitcoin		
			Host Fee: x%		
Transfer 5	Bitcoin address 5		Bitcoin address 4		
		From: Wallet B	To: Email address A		
		Amount in bitcoin	Amount in bitcoin		
			Miner's Fee = 0 bitcoin		
			Host Fee: 0 bitcoin		
Transfer 6	Bitcoin address 5		Bitcoin address 4		
		From: Wallet B	To: Email address A		
		Amount in bitcoin	Amount in bitcoin		
			Miner's Fee = 0 bitcoin		
			Host Fee: 0 bitcoin		
Transfer 7			Bitcoin address 4	Bitcoin address 6	
			To: Bitcoin Address 6	From: Wallet B (First Host)	
			Amount in bitcoin	Amount in bitcoin	
			Miner's Fee = 0.01 Bitcoin		
			Host Fee: 0 bitcoin		

Armstrong, Annotated Figure 45

To initiate a Bitcoin transaction, an application on a user device, illustrated in Figure 1B, “transmits a user interface request over the Internet 22 to the website 34” on a host computer. (CB-1006, ¶85; CB-1007, ¶36; CB-1008, ¶51.) User interface 36 provided by the website provides fields for entering information

regarding the bitcoin transaction (e.g., email address of party, amount of bitcoin, etc.). (CB-1006, ¶¶86; CB-1007, ¶37; CB-1008, ¶52.)

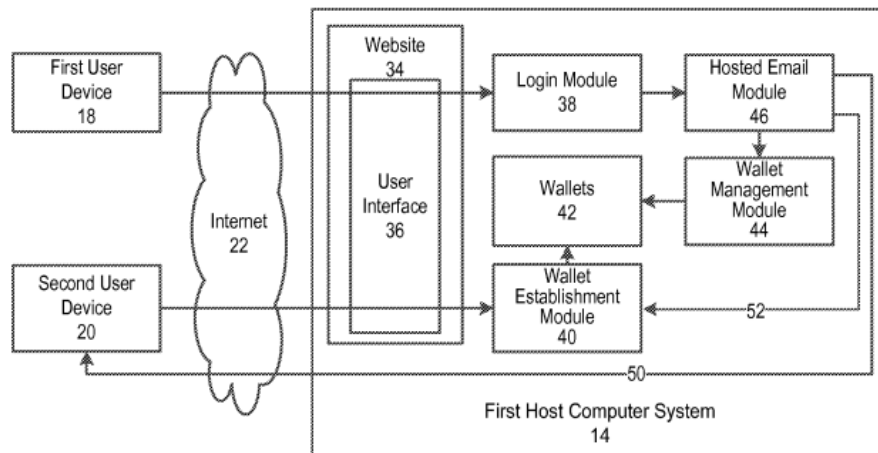


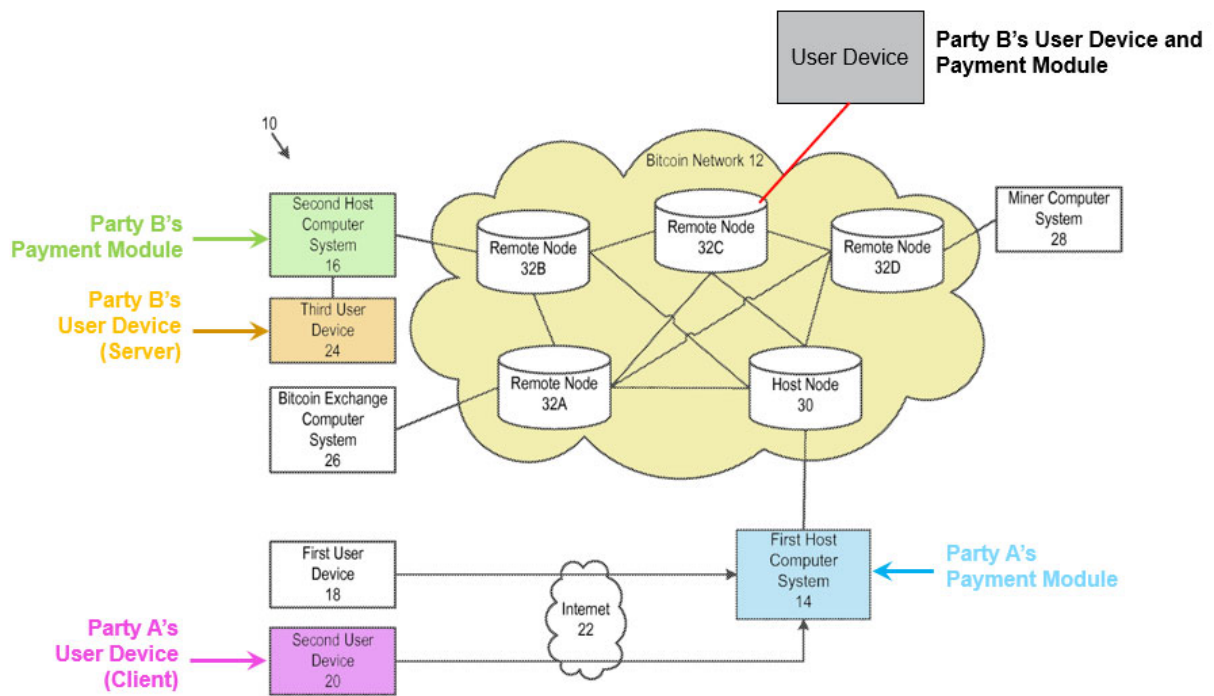
FIG. 1B

Armstrong, Figure 1B

3. Combination of Hearn and Armstrong

A POSITA would have been motivated to implement Hearn's distributed contracts, including micropayment contracts (Example 7), using Armstrong's Bitcoin network environment. (CB-1003, ¶¶79-85.) Specifically, as illustrated in annotated Figure 1A below, when implementing Hearn's Example 7, a host computer in Armstrong's network environment (e.g., first host computer 14) includes logic (software) necessary to handle Hearn's micropayment protocol including logic for processing the transactions specified in the protocol. (CB-1003, ¶79.) In a micropayment contract initiated by Party A with Party B, the first host computer (which hosts Party A's wallet) handles the client-side portion of the

protocol and processes transactions on behalf of Party A. (CB-1003, ¶¶79-80.) The component hosting Party B's wallet, and therefore acting as its payment module, handles the server-side portion of the protocol and processes transactions on behalf of Party B. Hearn teaches that Party B's user device acts as its payment module. (CB-1003, ¶80.) Armstrong teaches an embodiment where a host computer, coupled to a party's user device, acts as payment module for that party. (CB-1006, ¶103 (describing example transaction between a wallet held by first host computer and a wallet held by second host computer); CB-1007, ¶54; CB-1008, ¶69.) A POSITA would have understood Hearn's micropayment contract and Armstrong's architecture permits both options for a component acting as Party B's payment module. (CB-1003, ¶¶79-80, 90.) Figure 1A has been modified to include a user device (shaded gray) acting as Party B's payment module.



Armstrong, Annotated and Modified Figure 1A

A POSITA would have been motivated to combine Hearn with Armstrong for numerous reasons. (CB-1003, ¶¶81-85.) First, Hearn suggests the combination. (CB-1003, ¶81.) Hearn discloses its distributed contracts are “method[s] of using Bitcoin to form agreements with people via the block chain.” (CB-1009, 1.) However, Hearn does not provide details regarding a system architecture for performing its distributed contracts. (CB-1003, ¶81.) Moreover, Hearn does not indicate there is anything unique required for a Bitcoin architecture to implement its contracts. (*Id.*) A POSITA would have therefore been motivated to search for references describing Bitcoin network architectures and would have been led to

Armstrong which, like Hearn, is directed to Bitcoin and includes all the necessary components for implementing Hearn's contracts. (*Id.*) Moreover, both Armstrong and Hearn are in the same field as the '566 patent—systems and methods for use with decentralized digital currencies such as Bitcoin. (CB-1003, ¶82.)

Second, a POSITA would have been motivated to implement Hearn's distributed contracts, including Example 7's micropayments, using Armstrong's system to enhance the capabilities of the Armstrong's Bitcoin environment. (CB-1003, ¶83.) Specifically, Hearn describes that parties "want to rapidly and cheaply adjust the amount of money sent to a particular recipient without incurring the cost of a broadcast transaction." (CB-1009, 5.) Further, a POSITA would have recognized that transaction fees associated with existing credit/debit card payments systems make those payment methods impractical for micropayments. (CB-1003, ¶83.) Because of the need to provide an effective on-line method to pay for small dollar amount transactions, a POSITA would have been motivated to implement a micropayment technique within Armstrong's Bitcoin environment. (*Id.*)

Third, a POSITA would have been motivated to use Armstrong's web-based user interfaces and host computers, which facilitate Bitcoin transactions, to provide a simple mechanism for a user, such as Hearn's Party A, to enter into complex distributed Bitcoin contracts. (CB-1003, ¶84.) Additionally, the use of a facilitator (such as Armstrong's host computer) to handle processing involved in a Bitcoin

micropayment contract on behalf of an end-user allows for a more simplified payment application to be deployed and maintained on an end-user device. (*Id.*)

Finally, the combination is nothing more than applying a known technique (Hearn’s distributed contracts) to a known device (Armstrong’s Bitcoin environment and devices) ready for improvement. (CB-1003, ¶85.) The results of the combination would have been predictable to a POSITA because the combination merely involves the implementation of a protocol within the framework of the existing and known Bitcoin technology. (*Id.*) A POSITA would have had a reasonable expectation of success because, as noted by Hearn, a version of a micropayment protocol was implemented “in bitcoinj”⁹ and published prior to the ’566 patent. (*See* CB-1009, 5; CB-1003, ¶85.)

B. Claim 1

1. Preamble¹⁰ [1P]

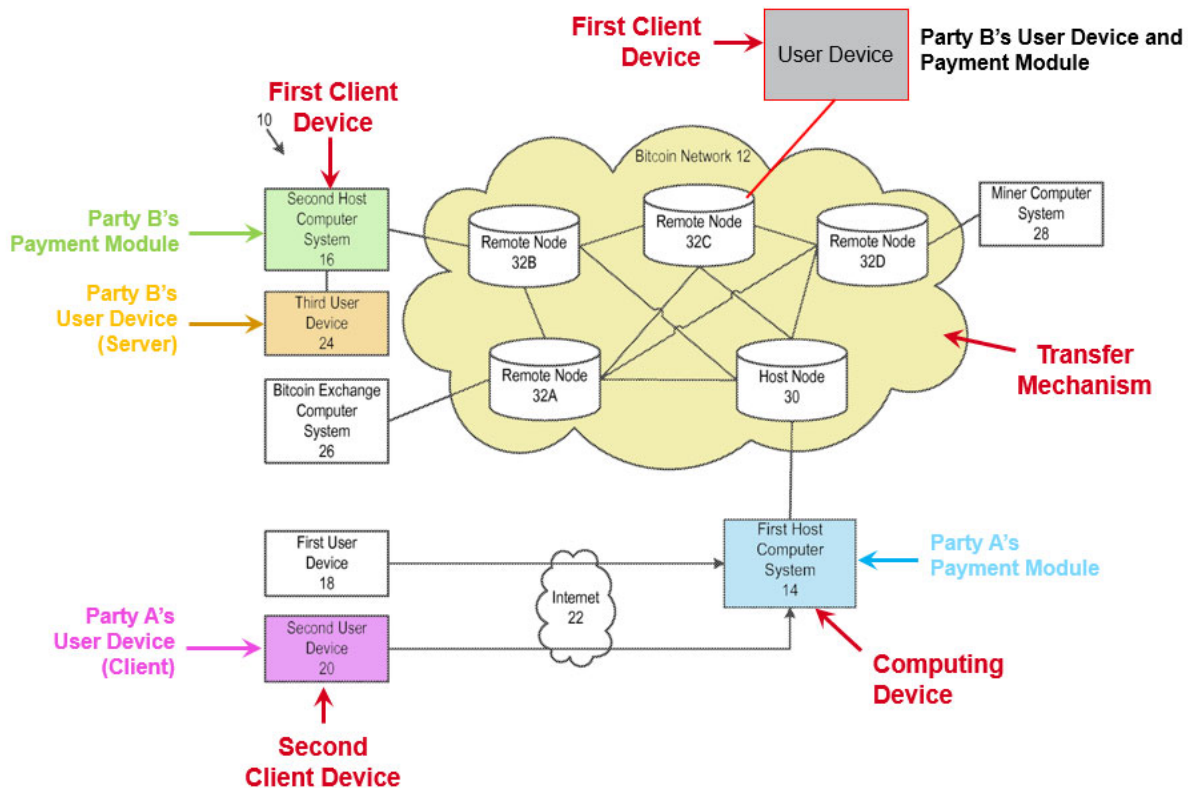
The combination of Hearn and Armstrong discloses a “*computing device for processing a transaction between a first client device, and a second client device*”

⁹ “bitcoinj” is a software library for working with the Bitcoin protocol. (CB-1003, ¶85.)

¹⁰ Petitioner does not acquiesce that the preamble is limiting.

via a transfer mechanism, the transfer mechanism comprising a decentralized digital currency” [1P]. (CB-1003, ¶¶87-93.)

Hearn’s Example 7 encodes a micropayment contract between two parties for the purchase of a service (e.g., Wi-Fi) on a per-usage basis using three Bitcoin transactions—an “escrow” (commit) transaction (T1), a refund transaction (T2), and a payment transaction (T3). (*See* CB-1009, 5; §V.A.1.) In the combined system of Hearn and Armstrong, illustrated below, Armstrong’s first host computer 14 (shaded blue) acts as the payment module for Party A, hosting Party A’s wallet. (CB-1003, ¶¶88, 79-80; §V.A.3; CB-1006, ¶8 (a host computer system “host[s] accounts or ‘wallets’ that allow users to make and accept payments using bitcoin”); CB-1007, ¶15; CB-1008, ¶15.) Armstrong’s host computer “is used primarily for transacting bitcoin.” (CB-1006, ¶83; CB-1007, ¶34; CB-1008, ¶49.) Armstrong’s first host computer 14 is therefore the “*computing device for processing a transaction.*” (CB-1003, ¶88.)



Armstrong, Annotated and Modified Figure 1A

In Armstrong, an application on a user device “transmits a user interface request over the Internet 22 to the website 34” on the host computer. (CB-1006, ¶85; CB-1007, ¶36; CB-1008, ¶51.) The second user device (shaded pink) is therefore the “*second client device*.” (CB-1003, ¶89.)

In Hearn, Party A enters a micropayment contract with Party B. Second host computer 16 hosts the wallet for Party B and acts as its payment module and therefore is the “*first client device*.” (CB-1003, ¶90.) Should PO incorrectly contend that host computer is not a “*client device*”, the combination further teaches that Party B’s user device acts as its payment module, as illustrated by the gray box

added by Petitioner to Figure 1A above. In this alternative, Party B's user device is the "*first client device*." (*Id.*) Party B's payment module operates in the same manner when Party B is the recipient of Hearn's micropayment contract, regardless of where it is physically located. (*Id.*)

In stage 2 of Hearn's micropayment protocol, first host computer 14, acting as the payment module for Party A, creates, signs, and sends an initial payment transaction T3 to the component acting as Party B's payment module. (CB-1009, 5 (step 7); CB-1003, ¶91; §V.A.1.) During the contract period between Party A and Party B, when "the client wishes to pay the server, it adjusts its copy of T3 to allocate more value to the server's output and less to its ow [sic]." (CB-1009, 5 (step 9).) The signed adjustments to T3 are provided by host computer 14 (Party A's payment module) to Party B's payment module (host computer 16 or Party B's user device) which then adjusts its copy of T3 "to match the new amounts." (*Id.*) The initial, incomplete version of T3 and the T3 updates are sent to Party B's payment module (second host computer 16 or Party B's device) over a communication medium such as the Internet. (CB-1003, ¶91.)

In Hearn's micropayment protocol (Example 7), "[w]hen the internet session ends or the predetermined time-period (e.g., 1-day) [for the contract] is close to expiring," the server "signs and **broadcasts** the last transaction it saw, allocating the final amount to itself." (CB-1009, 5; CB-1003, ¶92.) Armstrong explains that a

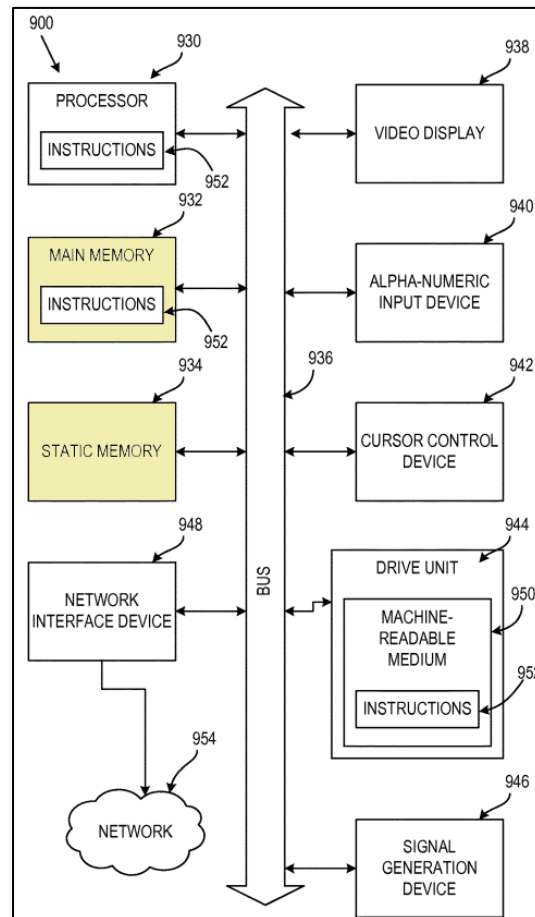
“transaction is broadcast to the Bitcoin network for block chain verification.” (CB-1006, ¶10; CB-1007, ¶7; CB-1008, ¶7.) Armstrong’s Bitcoin network 12 is therefore a “*transfer mechanism*.” (CB-1003, ¶92; CB-1001, 38:8-11.) Bitcoin was a well-known “*decentralized digital currency*” prior to the ’566 patent. (CB-1003, ¶92; CB-1001, 2:33-43 (Applicant’s Admitted Prior Art (“AAPA”) explaining “Bitcoin protocol and progeny (Ethereum, Litecoin, etc.) are one class” of “[d]ecentralized digital currencies”), 3:55-60, 36:62-67; *see also*, CB-1012, 1 (describing Bitcoin as a decentralized digital currency).)

The combination of Hearn and Armstrong therefore discloses a “*computing device* [first host computer 14 acting as payment module for Party A] *for processing a transaction* [e.g., payment transaction T3] *between a first client device* [payment module for Party B provided by second host computer 16 or Party B’s user device], *and a second client device* [second user device] *via a transfer mechanism* [Bitcoin network], *the transfer mechanism comprising a decentralized digital currency* [bitcoin].” (CB-1003, ¶¶87-93.)

2. “Memory” [1A]

The combination of Hearn and Armstrong discloses the “*computing device*” [first host computer] comprises “*a memory for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key*” [1A]. (CB-1003, ¶¶94-97.)

Armstrong discloses an exemplary computer system, illustrated in Figure 74 below including main memory 932 and static memory 934. (CB-1006, ¶226; CB-1007, ¶59, Figure 46; CB-1008, ¶94, Figure 54.) Each device in Armstrong’s network utilizes this “computer system” architecture. (CB-1006, ¶225 (computer system “operate[s] in the capacity of ... a peer machine in a peer-to-peer (or distributed) network environment”); CB-1007, ¶58; CB-1008, ¶93; CB-1003, ¶95.) Thus, the “*computing device*” includes “*a memory*” [1A]. (CB-1003, ¶95.)



Armstrong, Annotated Figure 74

The “*memory*” in the first host computer “*stor[es] a first asymmetric key pair.*” (CB-1003, ¶96.) In Armstrong, the wallet establishment module of the host computer “establishes a first wallet in the data store.” (See CB-1006, ¶16, ¶111 (“local register 60 includes a plurality of wallets 42”); CB-1007, ¶8; CB-1008, ¶¶9, 77.) The wallet further “stores the **public key of the Bitcoin address and its associated private key.**” (CB-1006, ¶8; CB-1007, ¶5; CB-1008, ¶5.) A POSITA would have understood the public/private key pair stored by Armstrong for a user’s wallet is an “*asymmetric key pair.*” (CB-1003, ¶96.) Asymmetric (or public-key) encryption algorithms were known for nearly 40 years before the ’566 patent. (See CB-1013, 4-5, 461.) In asymmetric encryption, keys “come in pairs”—a public key and corresponding private key, referred to as an asymmetric key pair. (CB-1003, ¶¶96, 34 *citing* CB-1013, 461, CB-1014, 4-5, 283.)

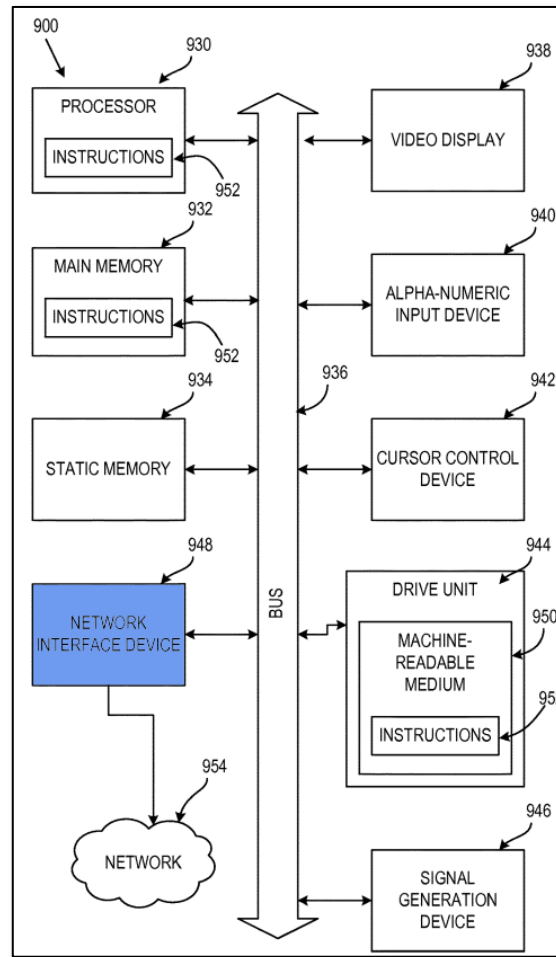
Hearn discloses its micropayment protocol uses public and private key pairs. (CB-1009, 5.) For example, in step 1, Party A “create(s) a public key (K1).” (CB-1009, 5 (step 1).) The process of creating the public key also creates an associated private key. (CB-1003, ¶97 *citing* CB-1013, 461, CB-1014, 4-5, 283.) Hearn further teaches Party A’s payment module signs transaction T3 with its private key and Party B’s payment module verifies the signature using Party A’s public key. (See CB-1009, 5 (steps 7-8); CB-1003, ¶97.) Thus, in the combination of Hearn and Armstrong, the first host computer acting as Party A’s payment module

includes “*memory for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key*” associated with Hearn’s Party A. (CB-1003, ¶¶94-97; CB-1001, 38:23-25 (AAPA explaining private keys are persistently stored).)

3. “*Network interface*” [1B]

The combination of Hearn and Armstrong discloses the “*computing device*” comprises “*a network interface for receiving*” data [1B]. (CB-1003, ¶¶98-100.)

Armstrong’s first host computer is connected over the Internet to second user device 20. (CB-1006, ¶81, Figure 1B (below); *see also*, ¶83; CB-1007, ¶¶32-34; CB-1008, ¶¶47-49.) The “computer system” used to implement Armstrong’s first host computer includes a “network interface device 948” [shaded blue] as shown in Figure 74 below. (CB-1006, ¶227, ¶16 (host computer system including “**a network interface device** connected to the processor”); CB-1007, ¶60, Figure 46; CB-1008, ¶95, Figure 54.)



Armstrong, Figure 74

In Armstrong, an application on the user device “transmits a user interface request” to website 34 on the host computer (CB-1006, ¶85; CB-1007, ¶36; CB-1008, ¶51.) Website 34 responds “by transmitting the user interface 36” to the user device. (CB-1006, ¶85; CB-1007, ¶36; CB-1008, ¶51.) User interface 36 provides fields for entering information regarding terms of a bitcoin transaction (e.g., amount of bitcoin, etc.). (CB-1006, ¶86; CB-1007, ¶37; CB-1008, ¶52.) For example, Armstrong’s Figure 42 shows “a view displayed to the user of the second

user device 20 ... to make a transfer from their wallet (Wallet B)” to another wallet, including entry of either an amount of Bitcoin or an amount in USD to transfer to another party. (CB-1006, ¶101; CB-1007, ¶52, Figure 42; CB-1008, ¶67, Figure 42.) Thus, the combination of Hearn and Armstrong discloses “a network interface for receiving” data [1B]. (CB-1003, ¶¶98-100.)

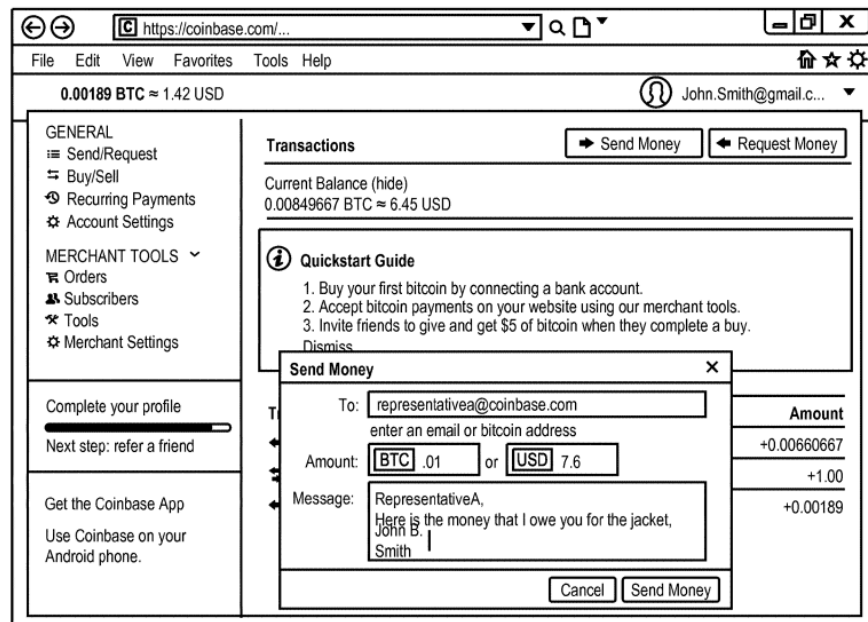


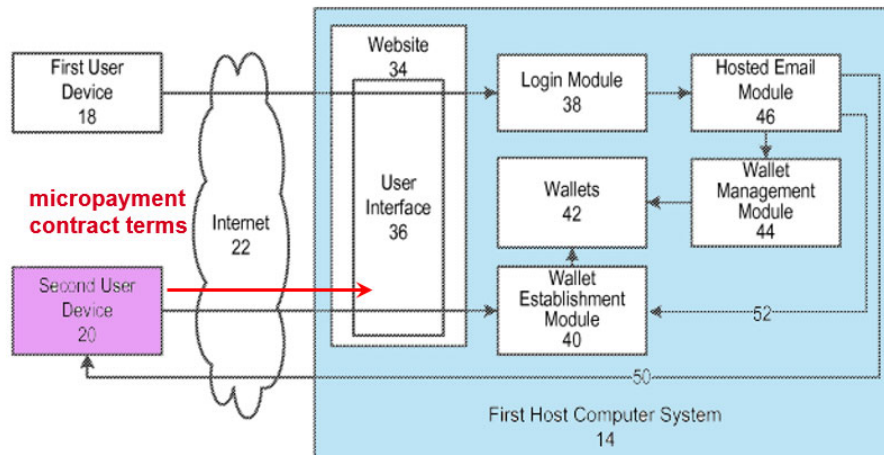
FIG. 42

Armstrong, Figure 42

4. “Term” [1B.1]-[1B.3]

Claim 1 recites the data received over the “network interface” are “terms” including “at least one of a first principal data or a second principal data” [1B.1]; “reference to at least one of a first data source or a second data source” [1B.2]; and “an expiration timestamp” [1B.3].

Hearn's Example 7 details a protocol for implementing a contract between Party A and Party B for a service offered by Party B (e.g., Wi-Fi access) using incremental, metered micropayments from Party A. To set up the micropayment contract, Party A must provide terms governing the agreement. These terms are received from the "*second user device*" over the "*network interface*" of the first host computer 14 ("computing device") in the combination of Hearn and Armstrong, as illustrated in annotated Figure 1B below. (CB-1003, ¶¶101-102.)



Armstrong, Annotated Figure 1B

a. "*Principal Data*" [1B.1]

In the combination of Hearn and Armstrong, the "*computing device*" receives "*at least one of a first principal data or a second principal data*" from Party A's user device (second user device). (CB-1003, ¶¶103-107.) During establishment of the payment channel between Party A and Party B, the payment module for Party A creates an "escrow" transaction (T1) specifying the **maximum**

anticipated value to be paid by Party A to Party B for the duration of the micropayment contract. (CB-1009, 5 (steps 1-2.)) This “maximum anticipated value” is specified by Party A and is the “*first principal data*.” (CB-1003, ¶104.) In Hearn’s Wi-Fi access example, Party A indicates via the user interface that it would “like to pay 0.001 BTC per 10 kilobytes of usage” with a maximum total payment of 10 BTC (100 Mbytes of usage) for the entire contractual period. (CB-1009, 5; CB-1003, ¶104.)

Armstrong discloses the originator of a transaction (e.g., Party A in Hearn’s micropayment contract) enters “either an amount in bitcoin (BTC) or an **amount in a local currency (USD-United States Dollar)**” into the user interface. (CB-1006, ¶101; CB-1007, ¶52; CB-1008, ¶67; *see also*, CB-1006, ¶86 (user interface includes “field for entering an amount in bitcoin (or an amount in local currency that is converted to bitcoin using an exchange rate”); CB-1007, ¶37; CB-1008, ¶52.) A POSITA would have been motivated to integrate the capability for a party initiating Hearn’s micropayment contract to enter the maximum payment amount for the contract in a local currency (e.g., USD), as taught by Armstrong. (CB-1003, ¶106.) For example, because of fluctuation of the exchange rate between bitcoin and local currencies combined with the limited use of digital currencies prior to the ’566 patent, a POSITA would have been motivated to provide a seller with the ability to offer a service in terms of a local currency and offer the ability for a

purchaser to pay using bitcoin. (*Id.*) For example, a café would have been motivated to offer Wi-Fi access on a per-usage basis for 0.01 USD for 10 kilobytes and allow payment of that amount in bitcoin. (*Id.*)

The combination further teaches the “*principal data*” is received via the “*network interface*.” (CB-1003, ¶108.) Because first host computer 14 processes contracts and their associated Bitcoin transactions for Party A, a POSITA would have understood the total maximum payment for the contract is a term entered via the user interface of Party A’s client device, as discussed above. (CB-1003, ¶107.) Armstrong discloses the amount to be transferred from the originating party (e.g., Party A) for a transaction is a field entered via the user interface 36 of the first host computer. (*See, e.g.*, CB-1006, ¶86 (user interface 36 includes “field for entering an **amount in bitcoin** (or an **amount in local currency** that is converted to bitcoin using an exchange rate) that is being transferred from the wallet”), 103 (User “enters a bitcoin address ... and **an amount of bitcoin to be transferred** to the third wallet”); CB-1007, ¶¶52, 54; CB-1008, ¶¶67-69.)

Thus, the combination of Hearn and Armstrong discloses the “*principal data*” (e.g., maximum contract value in either bitcoin or local currency) is received via the “*network interface*.” (CB-1003, ¶¶103-107.)

b. “Reference” to a “Data Source” [1B.2]

The local currency instrument (e.g., USD) entered with the principal data over the network interface is a “reference” to “a data source.” (CB-1003, ¶¶108-110; CB-1001, 11:55-56 (“a reference to a data source compris[es] at least one of: a base instrument and a quote instrument”), 11:66 (“Base: USD”), 11:67 (“Quote: AUD”).)

Armstrong’s user interface further presents the “exchange rate between bitcoin and the local currency.” (See CB-1006, Figure 42; CB-1007, Figure 42; CB-1008, Figure 42.) To support use of bitcoin when a seller provides pricing in a local currency, a POSITA would have been motivated to use an exchange rate to automatically convert an entered local currency amount to a bitcoin amount so that the user does not have to manually convert between a local currency and bitcoin and the parties can be confident the most recent exchange rate is being used and the conversion amount is accurate. (CB-1003, ¶109.) A POSITA would have understood the exchange rate used in Armstrong is provided from a “data source” such as an external feed from an exchange rate provider or a database internal to the first host computer. (*Id.*, citing CB-1012, 6-7 (identifying third party exchange rate providers); CB-1001, 15:38-49 (describing a “data source”).)

The combination of Hearn and Armstrong therefore teaches or suggests “a reference to at least one of a first data source or a second data source” is received over the “network interface” of the first host computer. (CB-1003, ¶¶108-110.)

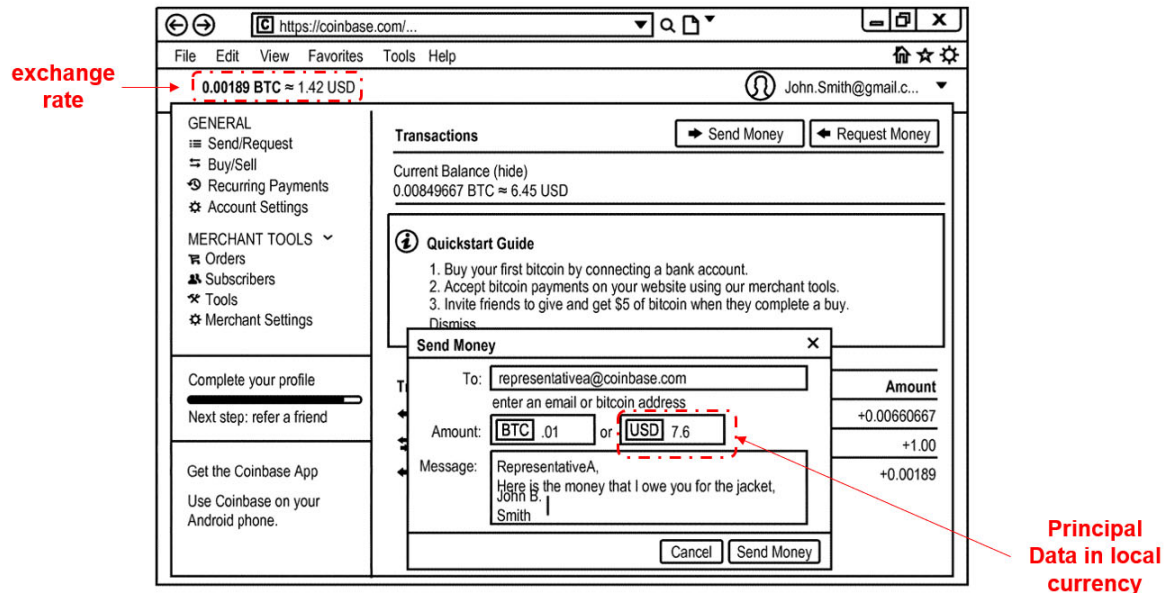


FIG. 42

Armstrong, Annotated Figure 42

c. “Expiration Timestamp” [1B.3]

The combination of Hearn and Armstrong teaches or suggests the “computing device” receives an “expiration timestamp” from Party A’s user device over the “network interface.” (CB-1003, ¶¶111-116.)

In Hearn, the micropayment channel between Party A and Party B **expires after a pre-determined time**, effectively ending the contract between the parties. (See CB-1009, 5 (“This continues until the session ends, or the 1-day period is getting close to expiry”).) When the time-period expires, Party A makes no further

micropayments and Party B accepts no further micropayments. (CB-1003, ¶112.)

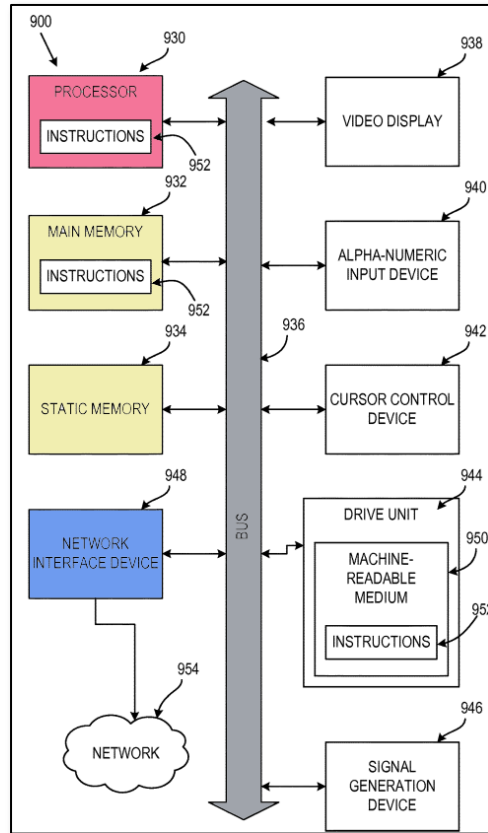
This pre-determined time-period sets the duration of the payment channel and is therefore an “*expiration timestamp*.” (CB-1009, 5.) A POSITA would have understood the expiration time of the channel occurs prior to when the refund transaction becomes spendable by Party A (i.e., prior to the lock time) to allow Party B sufficient time to broadcast the final payment transaction T3. (CB-1003, ¶113.) That is, the lock time for the refund transaction T2 is offset from the expiration time of the payment channel by a set amount. (*Id.*)

A POSITA would have been motivated to permit a user (e.g., Party A) to enter the duration of the micropayment channel (contract) as well as the refund lock time and/or time offset over the network interface with other contract terms (e.g., “*principal data*”) when the contract is being formed. (CB-1003, ¶114.) This feature provides parties with the flexibility to modify contract duration based on, for example, the type of service being provided or the level of trust between the parties. (*Id.*) For example, one user may wish to purchase internet access over a 2-hour period (e.g., from a café) whereas another user may wish to purchase internet access over a 24-hour period (e.g., from a hotel where the user is staying). (*Id.*) Indeed, the association of an expiration time/date for a contract between parties was well-known long before the ’566 patent. (CB-1003, ¶115; *see also*, CB-1015, ¶54; CB-1016, 16:28-29.)

5. “Computer Processor” [1C]

The combination of Hearn and Armstrong discloses the “*computing device*” comprises “*a computer processor coupled to the memory and the network interface*” [1C]. (CB-1003, ¶¶117-118.)

The computer system used to implement Armstrong’s first host computer, illustrated below, includes **processor 930** [shaded red] coupled to memory 932 [shaded yellow], memory 934 [shaded yellow], and network interface device 948 [shaded blue] via bus 936. (See CB-1006, ¶226-227, ¶16(“host computer ... including a **processor**, a network interface device connected to the processor, a computer readable medium connected to the processor, a data store on the computer readable medium”), CB-1006, ¶225; CB-1007, ¶¶59, 8, 58; CB-1008, ¶¶94, 9, 93.)



Armstrong, Annotated Figure 74

6. “Computer Processor” actions [1C.1]-[1C.4]

In the combination of Hearn and Armstrong, the first host computer (“*computing device*”) is configured to implement Hearn’s micropayment protocol including processing the required Bitcoin transactions (T1, T2, and T3). (See §V.A.3.) Accordingly, as detailed below, the combination of Hearn and Armstrong teaches or suggests the “*processor*” of the first host computer (“*computing device*”) is configured to perform the functions of “*read[ing] the first private ...*” [1C.1], “*computing a first cryptographic signature ...*” [1C.2], “*create[ing] an inchoate*

data record ...” [1C.3], and “*publish[ing] the inchoate data record ...*” [1C.4].

(CB-1003, ¶¶119-139.)

a. “***Read the First Private Key***” [1C.1] and “***Compute a First Cryptographic Signature***” [1C.2]

The combination of Hearn and Armstrong teaches “*read[ing] the first private key from the memory*” [1C.1] and “*comput[ing] a first cryptographic signature from the first private key*” [1C.2]. (CB-1003, ¶¶120-124.)

In Hearn’s Example 7, Party A “creates a new transaction, T3”, “**signs** T3”, and “provides the transaction and **signature** to the server” (Party B’s payment module). (CB-1009, 5 (step 7); CB-1003, ¶121.) Digital signatures were well-known and were a standard element of cryptographic applications long before the ’566 patent. (CB-1003, ¶¶122, 37.) A digital signature is created by computing a digest of content (e.g., by using a hash algorithm) and encrypting the digest using a party’s private key. (CB-1003, ¶37, *citing* CB-1013, 38.) The encrypted digest is a “*cryptographic signature*.” (CB-1003, ¶121.) Moreover, the ’566 patent admits, as it must, the use of digital signatures in Bitcoin transactions was known before its filing date. (*See* CB-1001, 4:30-31, 4:46-47, Figure 24 (AAPA describing use of digital signatures in Bitcoin); CB-1019, Abstract (identifying digital signatures as part of the solution to creating a peer-to-peer electronic cash alternative.)

Accordingly, Hearn teaches use of a “*private key*” to “*compute a first*

cryptographic signature” [1C.2] when creating the initial version of T3. (CB-1003, ¶¶121-122.)

As discussed in §V.B.2, the “*memory*” of Armstrong’s first host computer stores the “*private key*” and “*public key*” associated with Party A. The “*first private key*” of Party A therefore must be “*read*” from “*the memory*” for the processor to compute the digital signature for the initial version of transaction T3 created by Party A’s payment module (“*first host computer*”). (CB-1003, ¶¶123, 96-97.)

Accordingly, the combination of Hearn and Armstrong teaches “*read[ing] the first private key from the first private key*” [1C.1] and “*comput[ing] a first cryptographic signature from the first private key.*” (CB-1003, ¶¶120-124.)

b. “*Create an Inchoate Data Record*” [1C.3]

The combination of Hearn and Armstrong discloses “*create[ing] an inchoate data record*” [1C.3]. (CB-1003, ¶¶125-127.)

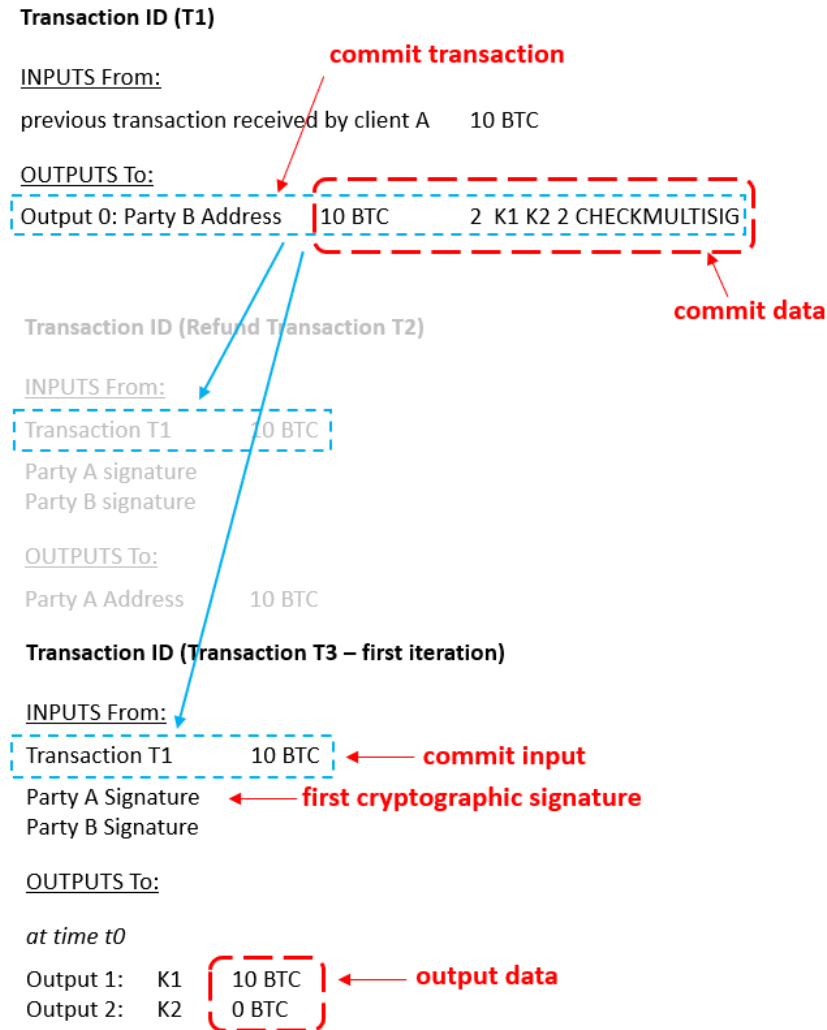
In the payment stage of Hearn’s micropayment protocol, Party A “creates a new transaction, T3” which allocates the entire maximum payment value to Party A and nothing to Party B. (CB-1009, 5(step 7).) Periodically, during the micropayment contract between the parties (as set by the expiration timestamp), transaction T3 is adjusted by Party A to assign more of the payment to Party B and less to Party A and “re-signed.” (CB-1009, 5 (step 9).) The process of adjusting T3

“continues until the session ends, or the 1-day period is getting close to expiry.”

(*Id.*) Party B then “signs and broadcasts the last transaction it saw, allocating the final amount to itself.” (*Id.*) At this point, transaction T3 is complete. The initial version of T3 created in step 7 is an “*inchoate data record*” because it is unsigned by the receiving party (Party B) and therefore is not fully formed. (CB-1003, ¶126, *citing* CB-1017, 966 (defining “inchoate” as not fully formed).)

(i) “Commit Input” [1C.3a]

The initial version of T3 includes “*a commit input for receiving a commit data from a commit transaction*” [1C.3a]. (CB-1003, ¶¶129-131.) As acknowledged in the AAPA of the ’566 patent, “a transaction must have one or more inputs.” (CB-1001, 4:42-43, 49.) For a Bitcoin transaction to be valid, “every input must be an unspent output of a previous transaction.” (CB-1001, 4:45-46 (AAPA); *see also*, CB-1006, Figure 45 (illustrating each transaction uses previous transaction output as input); CB-1007, ¶¶54-57; CB-1008, ¶¶69-72.) Hearn’s transaction T3 “connects to T1.” (CB-1009, 5 (step 7).) That is, the unspent output of “escrow” transaction T1 is the “*input*” for the initial payment transaction T3 as shown in Miller Figure C below. (CB-1003, ¶¶129-130.)



Miller, Figure C

As discussed in §V.A.1, “escrow” transaction T1 “sets up a payment of (for example) 10 BTC to an output requiring both the server’s public key and one of” the client to be used. (CB-1009, 5 (step 2).) After both parties sign “escrow” transaction T1 (step 6), “escrow” transaction T1 is “broadcast[]” to the Bitcoin network which commits T1 to the blockchain and “locks” in the bitcoin. (CB-1009, 5 (step 6).) Thus, “escrow” transaction T1 is a “*commit transaction*” because it

commits Party A to transfer an amount of BTC (the “*commit data*”). (CB-1003, ¶131.) Hearn’s initial payment transaction T3 therefore includes “*a commit input for receiving a commit data from a commit transaction*” [1C.3a]. (CB-1003, ¶¶129-131.)

(ii) “*One or More Output Data*” [1C.3b]

The initial version of T3 includes “*one or more output data obtained from at least one of the first principal data or the second principal data, and a value data from at least one of the first data source or the second data source*” [1C.3b]. (CB-1003, ¶¶132-135.) Hearn’s initial payment transaction T3 has “two outputs”¹¹—one goes to Party A and one goes to Party B. (CB-1009, 5 (step 7).) Transaction T3 “starts with all value allocated to the first output” (e.g., 10 BTC are assigned to Party A and 0 assigned to Party B). (*Id.*) The “two outputs” (BTC amounts) of the initial version of transaction T3 are “*one or more output data*” [1C.3b]. (CB-1003, ¶¶133-134.)

As discussed in §V.B.4.a, the “*principal data*” for Hearn’s Example 7 are received in local currency (e.g., U.S. Dollars) in the combination of Hearn and

¹¹ A POSITA would have understood the output also includes a “miner’s fee.” (CB-1003, ¶133, *citing* CB-1001 (AAPA), 4:55-56; CB-1006, ¶103; CB-1007, ¶56; CB-1008, ¶71.)

Armstrong. As taught by Armstrong, “an amount in local currency [] is converted to bitcoin using an exchange rate.” (CB-1006, ¶86; CB-1007, ¶52; CB-1008, ¶67.)

An exchange rate is “*a value data from at least one of the first data source*”

(exchange rate provider or internal exchange rate database). (CB-1003, ¶134.)

Thus, “*one or more output data*” in the combination of Hearn and Armstrong is

“*obtained from at least one of the first principal data [maximum contract amount in local currency] ... and a value data [exchange rate] from at least one of the first*

data source [exchange rate provider or internal database]” [1C.3b]. (CB-1003,

¶¶134-135.)

(iii) “*First Cryptographic Signature*” [1C.3c]

The initial version of T3 includes “*the first cryptographic signature*”

[1C.3c]. (CB-1003, ¶136.) In Hearn’s Example 7, the “client signs T3 and provides

the transaction and **signature** to the server.” (CB-1009, 5 (step 7).)

c. “*Publish the Inchoate Data Record*” [1C.4]

The combination of Hearn and Armstrong discloses “*publish[ing] the inchoate data record to at least one of the first client device or the second client device*” [1C.4]. (CB-1003, ¶¶137-139.)

After initial version of T3 (“*the inchoate data record*”) is created, the first host computer “signs T3” using Party A’s private key and “**provides the transaction and signature to the server.**” (CB-1009, 5 (step 7).) In the

combination of Hearn and Armstrong, initial payment transaction T3 is provided with the signature to Party B's payment module (e.g., the second host computer or to Party B's user device; "*first client device*"). (CB-1003, ¶138.) Sending the initial version of the payment transaction T3 to the component acting as Party B's payment module "*publish[es] the inchoate data record*" because "publish[ing] [a] transaction record to [a device]" in the '566 patent "[m]ak[es] the transaction record available for reading or copying by the device, for example, **by sending the transaction record to the device** via a network interface." (CB-1001, 37:23-35; CB-1003, ¶¶137-138.)

The combination of Hearn and Armstrong therefore discloses the "*processor*" of the "*computing device*" [first host computer] "*publish[es] the inchoate data record to ... the first client device* [component acting as Party B's payment module]" [1C.4]. (CB-1003, ¶¶137-139.)

7. "*Distributed Ledger*" [1D]

The combination of Hearn and Armstrong discloses "*the decentralized digital currency comprises a distributed ledger that enables processing the transaction between the first client device and the second client device without the need for a trusted central authority*" [1D]. (CB-1003, ¶¶140-144.) It was well-known that Bitcoin is a decentralized peer-to-peer network using a public transaction ledger (blockchain). (See §V.B.1; CB-1003, ¶141 *citing* CB-1012, 1-3;

CB-1019, Abstract.) Armstrong explains that in Bitcoin, when a transaction is made between different host computer systems, “the transaction is broadcast to the Bitcoin network for **block chain verification**.” (CB-1006, ¶10; CB-1007, ¶7; CB-1008, ¶7.) Specifically, “[p]articipants known as ‘miners’ at miner computer systems verify and timestamp transactions into a shared public database called a ‘block chain’.” (CB-1006, ¶7; CB-1007, ¶4; CB-1008, ¶4.) And as acknowledged by the ’566 patent, the blockchain is a “public ledger” (“distributed database”) that “records bitcoin transactions” without the need for “any trusted central authority.” (CB-1001, 3:63-64 (AAPA), 4:5 (AAPA); *see also*, CB-1003, ¶143 *citing* CB-1012, 9.)

Because Hearn’s micropayment protocol broadcasts two transactions to the Bitcoin network (complete T1 and final, complete T3), “*the decentralized digital currency [bitcoin] comprises a distributed ledger [blockchain] that enables processing the transaction [payment transaction T3] between the first client device and the second client device without the need for a trusted central authority*” [1D]. (CB-1003, ¶¶140-144; §V.A.1.)

8. “Create a Complete Data Record” [1E]

The combination of Hearn and Armstrong discloses “*the inchoate data record is used by at least one of the first client device or the second client device to create a complete data record*” [1E]. (CB-1003, ¶¶145-147.)

In the payment stage of Hearn’s micropayment protocol as implemented in Armstrong, the first host computer, acting as Party A’s payment module, sends the initial version of payment transaction T3 (“*inchoate data record*”) to the component acting as Party B’s payment module (second host computer or Party B’s user device). (CB-1009, 5 (step 7); CB-1003, ¶146.) The first host computer device then “adjusts its copy of T3 to allocate more value to the server’s output and less to its ow [sic]” as Party A consumes the service offered by Party B. (CB-1009, 5 (step 9).) The first host computer “re-signs the new T3” using Party A’s private key and “sends the signature to the server.” (*Id.*) The component acting as Party B’s payment module then “adjusts its copy of T3 to match the new amounts, verifies the signature and continues.” (*Id.*) This incremental payment process “continues until the session ends” or the period set by the expiration timestamp “is getting close to expiry.” (*See* CB-1009, 5.) At that point, Party B’s payment module “**signs and broadcasts** the last transaction it saw, allocating the final amount to itself.” (*Id.*) The final version of T3 signed by both parties and broadcast to the Bitcoin network for verification is a “*complete data record*.” (CB-1003, ¶146.) Thus, the component acting as Party B’s payment module (“*the first client device*”) “*create[s] a complete data record*” from the initial version of T3 (“*inchoate data record*”). (*Id.*)

In the combination of Hearn and Armstrong, the component acting as Party B's payment module "*creat[es] the transaction by broadcasting the complete data record for transmitting and receiving among network participants in the computer network for recording in the distributed ledger*" [1E]. (CB-1003, ¶147.) As discussed above, Party B's payment module "broadcasts" the final version of T3 to the Bitcoin network for verification. (CB-1009, 5; CB-1006, ¶10; CB-1007, ¶7; CB-1008, ¶7.) Specifically, as part of blockchain verification, miners "verify and timestamp transactions into a shared public database called a 'block chain'." (CB-1006, ¶7; CB-1007, ¶4; CB-1008, ¶4.) After the transactions are added to the ledger, the additions are communicated to other nodes. (See, CB-1006, ¶102; CB-1007, ¶53; CB-1008, ¶68; CB-1001, 3:63-4:5 (AAPA related to blockchain).)

9. "Sign[]" and "Save a Copy of the Inchoate Data Record" [1F]

The combination of Hearn and Armstrong discloses "*at least one of the first client device or the second client device signs the inchoate data record and saves a copy of the inchoate data record on at least one of the first client device or the second client device*" [1F]. (CB-1003, ¶¶148-150.)

In Hearn's Example 7, after Party B receives the initial version of payment transaction T3, the first host computer ("*computing device*") adjusts its copy of T3 and sends "the signature and the amount to increment" to Party B. (CB-1009, 5 (step 9).) Party B then "adjusts **its copy of T3** to match the new amounts." (*Id.*)

That is, the component acting as Party B’s payment module stores a copy of the initial version of T3 (“*inchoate data record*”) locally so that it can be updated when incremental payments are received from Party A. Thus, in the combination of Hearn and Armstrong, the component acting as Party B’s payment module (second host computer or Party B’s user device; “*first client device*”) “*saves a copy of the inchoate data record on at least one of the first client device ...*” [1F]. (CB-1003, ¶149.)

At the end of the contract, Party B’s payment module “**signs and broadcasts** the last transaction” (i.e., the final version of T3) to the Bitcoin network. (CB-1009, 5; CB-1003, ¶150.) Thus, in the combination of Hearn and Armstrong, the component acting as Party B’s payment module (second host computer or Party B’s user device) also “*signs the inchoate data record*” [1F]. (CB-1003, ¶150.)

10. “*Verif[y] the Recording of the Complete Data Record in the Distributed Ledger*” [1G]

In the combination of Hearn and Armstrong, both the first host computer (“*the computing device*”) and the component acting as Party B’s payment module (“*the first client device*”) “*verif[y] the recording of the complete data record in the distributed ledger by observing an external state*” [1G]. (CB-1003, ¶¶151-153.)

As part of blockchain verification, “‘miners’ at miner computer systems verify and timestamp transactions into a shared public database called a ‘block

chain’.” (CB-1006, ¶7; CB-1007, ¶4; CB-1008, ¶4.) In Armstrong, a “block chain verification notice” is broadcast by miner computer system 28. (CB-1006, ¶102; CB-1007, ¶53; CB-1008, ¶68.) Party A’s payment module, first host computer, (the “*computing device*”) and Party B’s payment module (“*first client device*”) monitor for these notices and determine whether to change a “marker” for a transaction, such as payment transaction T3, from ““PENDING” to ‘COMPLETE’” as shown in Figure 43 below. (CB-1006, ¶102; CB-1007, ¶53, CB-1008, ¶68.) The notice, originating for a source external to the host, provides “*an external state*” indicating whether the “*complete data record*” (final T3) has been recorded in the blockchain. (CB-1003, ¶152.) By monitoring for these notices and reviewing their contents, the first host computer system and the component acting as Party B’s payment module “*observe*” the “*external state*” reflective of whether the transaction was recorded in the blockchain—i.e., by “*observing*” the “*external state*” it “*verifies the recording of the complete data record in the distributed ledger.*” (*Id.*)

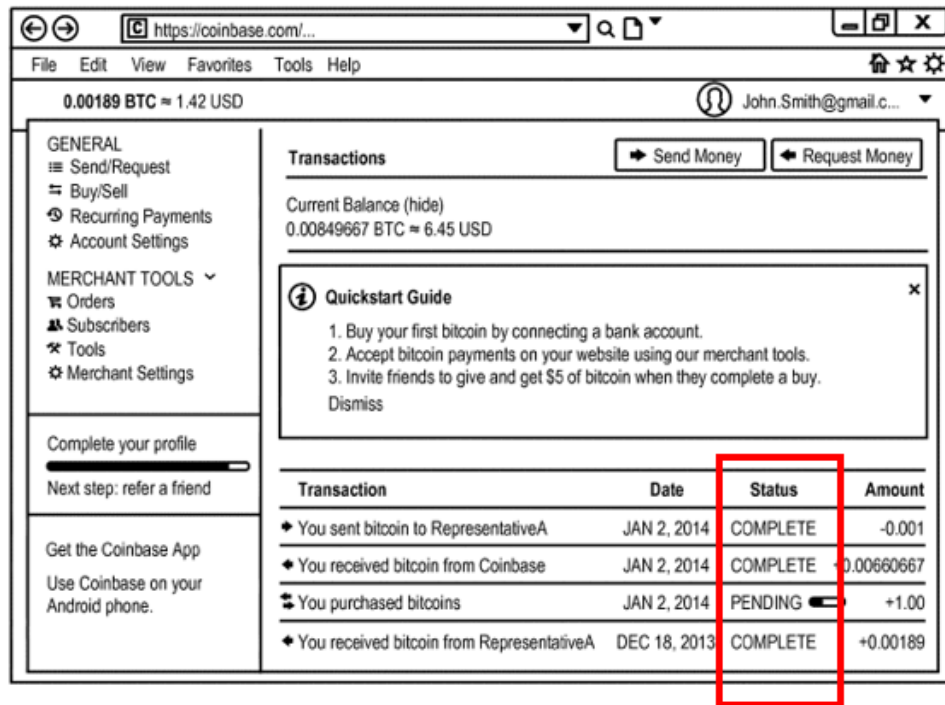


FIG. 43

Armstrong, Annotated Figure 43

C. Dependent Claim 2

Claim 2 narrows limitation [1C.3b] by specifying “*the one or more output data*” is obtained from “*the first principal data*” rather than either the “*first principal data or the second principal data*” and from “*the value data from the first data source*” rather than “*the value data from the first data source or the second data source.*” Petitioner established in §V.B.6.ii “*output data*” is obtained from the “*first principal data*” and “*value data from the first data source.*” For the reasons set forth in §V.B.6.ii, the combination of Hearn and Armstrong also renders claim 2 obvious. (CB-1003, ¶154.)

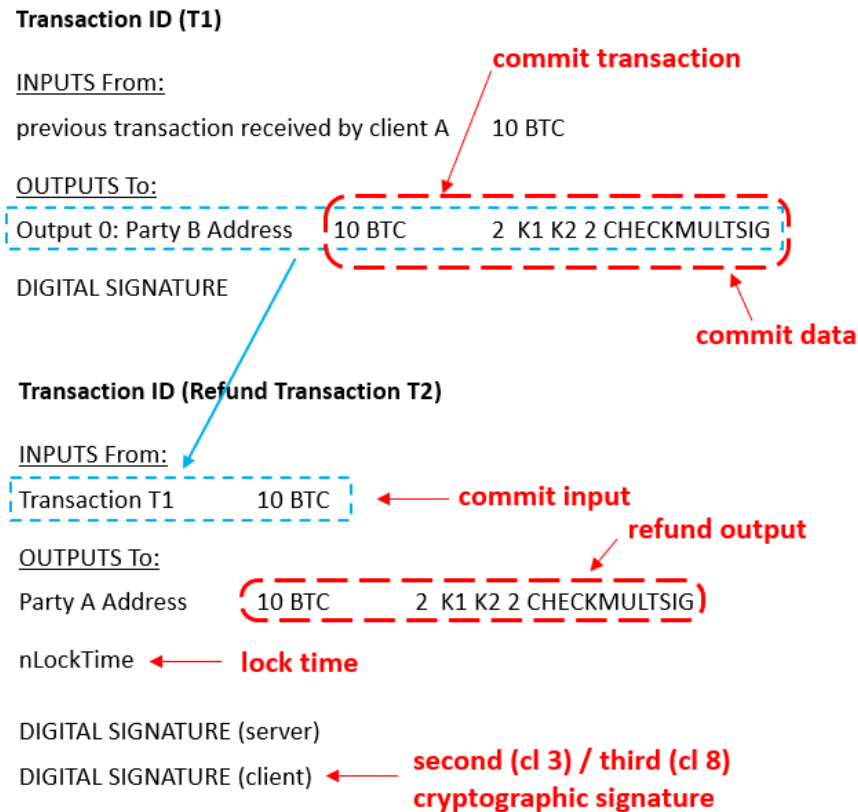
D. Dependent Claim 3

Claim 3 is directed to a refund transaction. Petitioner addresses the limitations of claim 3 starting with limitation [3B].

The combination of Hearn and Armstrong discloses the “*computer processor*” of the first host computer “*creat[es] another inchoate data record*” [3B]. (CB-1003, ¶¶156-164.) As discussed in §V.A.1, parties to a micropayment contract collaborate to create a signed refund transaction, T2, that spends the maximum payment value for the contract back to Party A. Specifically, after creation of “escrow” transaction T1, the first host computer (“*computing device*”) creates a refund transaction (T2) “which sends all the money back” to Party A. (CB-1009, 5 (step 3).) Refund transaction T2 is an “*inchoate data record*” until it is signed by both parties, the time lock for the transaction expires, and the transaction is broadcast to the Bitcoin network for verification. (CB-1003, ¶156.)

Hearn’s transaction T2 “is connected to T1.” (CB-1009, 5 (step 3).) That is, the unspent output of “escrow” transaction T1 is the “*input*” for the refund transaction, as illustrated in Miller Figure D below. (CB-1003, ¶157.) As discussed in §V.B.6.b, “escrow” transaction T1 is a “*commit transaction*” because it commits Party A to transfer an amount of BTC (the recited “*commit data*”). (CB-1003, ¶157.) Refund transaction T3 therefore also includes “*a commit input for receiving a commit data from the commit transaction*” [3B.1]. (*Id.*)

Because refund transaction T2 “sends all the money” from the “escrow” transaction “back” to Party A, the value of the maximum total payment for the contract specified in T1 is also the output value in the refund transaction. (See CB-1009, 5 (step 3).) Thus, refund transaction T2 includes “a refund output comprising a refund data” [3B.2]. (CB-1003, ¶158.)



Miller, Figure D

Hearn’s refund transaction also includes a “time lock set for some time in the future, for instance a few hours.” (CB-1009, 5.) Thus, refund transaction T2 includes “a lock time” [3B.4]. (CB-1003, ¶159.)

Because the input of the refund transaction is tied to the output of T1, the output of refund transaction T2 requires “**two signatures to be spent**”—the signature of Party A and signature of Party B. (CB-1009, 5 (steps 3-4).) The first host computer obtains Party B’s signature by sending T2 to Party B which “signs T2” and “returns the signature to the client” (step 4). (CB-1003, ¶160.) Hearn teaches that Party A “can broadcast the refund transaction and get back all the money.” (*Id.*) A POSITA would understand Party A must sign the refund transaction before the refund transaction is broadcast or the transaction would be deemed invalid by the Bitcoin network. (*Id.*) Accordingly, refund transaction T2 includes a “*second cryptographic signature*” [3B.3] and the “*computer processor*” of the first host computer (“*the computing device*”) must “*compute a second cryptographic signature from the first private key*” [3A] of Party A. (*Id.*)

The first host computer holds signed refund transaction T2 until certain conditions are met, including the expiration of the time lock. (CB-1009, 5.) Thus, T2 remains incomplete. (CB-1003, ¶161.) For example, Hearn teaches the refund transaction is only finalized by broadcasting T2 to the Bitcoin network in cases “where the server disappears or halts at any point, leaving the allocated value in limbo.” (CB-1009, 5.) Thus, in the combination of Hearn and Armstrong, the first host computer (“*computing device*”) identifies when the server becomes unavailable or uncooperative during the micropayment contract. (*Id.*) A POSITA

would have been motivated to inform Party A of the circumstance by posting the pending refund transaction when a server failure is identified. (CB-1003, ¶162.) Alternatively, a POSITA would have been motivated to simply post the status of a refund transaction until expiration of the contract. (*Id.*) A pending refund would simply be cancelled if the contract completes successfully. (*Id.*) Armstrong supports such notification, teaching the host computer provides a webpage displaying to a user “transactions that have been initiated or completed.” (CB-1006, ¶102; CB-1007, ¶53; CB-1008, ¶68.) A POSITA would have been motivated to display the refund transaction T2 on this page as pending when the client reports non-performance or during every micropayment contract so the user can track the status of the refund of its committed payment. (CB-1003, ¶163.) The posting of the refund occurs during the contractual time period and before the lock time expires. (*Id.*)

The display of a pending refund transaction is based on the contents of the “*inchoate data record*” associated with T2 and “*publish[es] the another inchoate data record*” because the inchoate data record is stored in a way that permits the record to be read by the client device associated with Party A (“*the second client device*”). (CB-1003, ¶164; CB-1001, 37:23-31 (describing the term “publish[ing]”).) Thus, the combination of Hearn and Armstrong renders obvious

“publish[ing] the another inchoate data record to at least one of the first client device or the second client device” [3C]. (CB-1003, ¶164.)

VI. GROUND 2: COMBINATION OF HEARN, ARMSTRONG, AND ZIEGLER RENDERS CLAIMS 7-8 OBVIOUS

Independent claim 7 includes substantially overlapping subject matter with independent claim 1 as detailed below. The combination of Hearn and Armstrong teaches or suggests every limitation of claim 1. (*See* §V.B.) The combination does not explicitly disclose the *“second client device”* includes a memory for *“storing a third asymmetric key pair”* [7C.1] and a processor *“configured to read the third private key from the third memory”* [7C.3]. However, the storage and use of private keys in a networked device were well-known and taught by Ziegler.

A. Overview of the Combination

1. Ziegler

Ziegler relates to “secure information transfer.” (CB-1010, 1:12-13.)

Ziegler’s information transfer system, illustrated in Figure 2, includes computer 102 coupled to Web server 120 which provides an interface to application server 122 “connected to a host cryptographic module 124” (“Host”). (CB-1010, 3:33-37.)

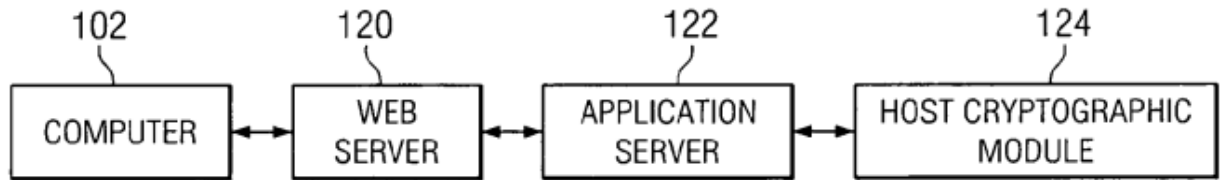


FIG. 2

Ziegler, Figure 2

After a user accesses a website, an “SSL secured session is established between the Web server and the client PC” and the system’s software is downloaded “and installed on the client.” (CB-1010, 4:31-40.) Next, an “RSA Public/Private Key pair (1024) is generated” at the client. (CB-1010, 4:47-48.) The Public Key is sent to the Web Server and shared with the Application server and Host. (CB-1010, 4:48-50.) The Public/Private Key pair for the client is subsequently used to establish session (symmetric) keys for communication between the client and server. (CB-1010, 4:46-47.)

Specifically, the Host generates communications and data symmetric keys. (CB-1010, 4:50-55.) The Host further creates two cryptograms—(1) the communications key and a hash of the communication key, encrypted (wrapped) with the client’s RSA public key and (2) the data key and a hash of the data key, encrypted (wrapped) with the client’s RSA public key and encrypted with the communications key. (CB-1010, 4:56-67.) The Host then combines these two cryptograms, “generates a cryptographic hash”, encrypts the combination and its

hash with the client's public key, and sends this resulting cryptogram (referred to as the "key package") to the client. (CB-1010, 5:1-9.)

The client first "decrypts the key package with its Private Key" to obtain the two cryptograms. (CB-1010, 5:10-11.) The client decrypts the first cryptogram using its private key and verifies its integrity. (CB-1010, 5:17-21.) The client then decrypts the second cryptogram with the communications key and with the client's private key and verifies its integrity. (CB-1010, 5:21-26.) The client now has the communications key and data key "for further communication with the Application Server" during a session. (CB-1010, 5:26-28.)

2. Combination of Hearn, Armstrong, and Ziegler

A POSITA would have been motivated to use Ziegler's secure information transfer technique for communication between Armstrong's second user device ("*second client device*") and the host computer in the combined system of Hearn and Armstrong, discussed in §V.A.3. (CB-1003, ¶¶170-173.)

Financial transactions were and remain frequent targets of fraud. (CB-1003, ¶171.) A POSITA would have therefore been motivated to combine Ziegler with Hearn and Armstrong to provide secure communications for financial transactions between a user device and the host computer to prevent fraud and/or disclosure of client confidential information. (*Id.*) Ziegler further suggests the combination, noting "[a]ny system implementing an electronic transfer of funds, for example,

requires multi-level security measures.” (CB-1010, 1:19-21; CB-1003, ¶172.)

Specifically, “transactions between strangers and more particularly, transactions conducted on an open-network like the Internet cannot be conducted within reasonable risk limitations without some kind of identity verification.” (CB-1010, 1:28-31.) Because Armstrong uses a web application which communicates financial information between a user device and the host over the Internet and Hearn’s contract are designed for use between strangers (trustless transactions), a POSITA would have been motivated to incorporate additional communications security to remove risks. (CB-1003, ¶172.)

The combination of Ziegler with Hearn and Armstrong is merely the combination of a known technique (Ziegler’s secure communication technique) to improve similar devices (systems for transacting financial transactions) in the same way (use of secure communications). (CB-1003, ¶173.) The results of the combination would have been predictable because secure communication protocols were well known and in use long before the ’566 patent. (*Id.*)

B. Independent Claim 7

Claim 7 recites “*a system for processing a transaction between a first client device and a second client device*” [7P]. The system recites limitations directed to “*the computing device*” [7A], “*the first client device*” [7B], and “*the second client*

device” [7C]. The combination of Hearn, Armstrong, and Ziegler renders claim 7 obvious.

1. Preamble [7P]

Petitioner established in §V.B.1 the combination of Hearn and Armstrong discloses a “computing device for processing a transaction between a first client device, and a second client device via a transfer mechanism” [1P]. For the reasons discussed in §V.B.1, the combination of Hearn and Armstrong also discloses a “system for processing a transaction between a first client device and a second client device via a transfer mechanism, the system comprising a computing device, the first client device, the second client device, and the transfer mechanism” [7P]. (CB-1003, ¶175.)

2. “Computing Device” [7A]

Claim 7’s “computing device” limitations [7A.1]-[7A.3] are identical to claim 1’s limitations [1A]-[1C], as set forth in the table below. For the reasons set forth in the cited sections, the combination of Hearn and Armstrong renders the “computing device” limitations obvious. (CB-1003, ¶176.)

[7A.1] first memory ...	See §V.B.2 [1A]
[7A.2] first network interface ... the terms comprising:	See §V.B.3 [1B]
[7A.2a] first principal ...	See §V.B.4.a [1B.1]
[7A.2b] reference to ... first data source ...	See §V.B.4.b [1B.2]

[7A.2c] <i>expiration timestamp</i>	<i>See §V.B.4.c [1B.3]</i>
[7A.3] <i>first computer processor ... configured to:</i>	<i>See §V.B.5 [1C]</i>
[7A.3a] <i>read the first private key ...</i>	<i>See §V.B.6.a [1C.1]</i>
[7A.3b] <i>compute first cryptographic signature ...</i>	<i>See §V.B.6.a [1C.2]</i>
[7A.3c] <i>create inchoate data record comprising;</i>	<i>See §V.B.6.b [1C.3]</i>
[7A.3c.i] <i>commit input ...</i>	<i>See §V.B.6.b.i [1C.3a]</i>
[7A.3c.ii] <i>one or more outputs [and] value data ...</i>	<i>See §V.B.6.b.ii [1C.3b]</i>
[7A.3c.iii] <i>first cryptographic signature; and</i>	<i>See §V.B.6.b.iii [1C.3c]</i>
[7A.3d] <i>publish inchoate data record ...</i>	<i>See §V.B.6.c [1C.4]</i>

3. “First Client Device” [7B]

a. “Memory” [7B.1], “Network Interface” [7B.2], and “Computer Processor” [7B.3]

As discussed in §V.B.1, the second host computer which acts as Party B’s payment module is the “*first client device*.” (CB-1003, ¶178.) Should PO incorrectly contend that host computer is not a “*client device*”, the combination further teaches that Party B’s user device acts as its payment module. In this alternative, Party B’s user device is the “*first client device*.” (*Id.*) Party B’s payment module operates in the same manner when Party B is the recipient of Hearn’s micropayment contract, regardless of where it is physically located. (*Id.*)

Each device in Armstrong’s network, including the second host computer and stand-alone user devices, utilize the “computer system” architecture illustrated in Figure 74. (CB-1006, ¶225 (machine “may operate in the capacity of ... a peer machine in a peer-to-peer (or distributed) network environment”), ¶226; CB-1007, ¶58; CB-1008, ¶93; CB-1003, ¶178.) The computer system includes main memory 932 and static memory 934, network interface device 948, and processor 930 coupled to memory 932, memory 934, and network interface device 948 via bus 936. (See CB-1006, 226-227; CB-1007, ¶¶59-60; CB-1008, ¶¶94-95.)

Thus, Armstrong discloses the “*first client device*” comprises “*a second memory*” [7B.1], “*a second network interface*” [7B.2], and “*a second computer processor coupled to the second memory and the second network interface*” [7B.3]. (CB-1003, ¶¶177-179.)

The “*memory*” in the component acting as Party B’s payment module “*stor[es] a second asymmetric key pair.*” (CB-1003, ¶180.) As discussed in §V.B.2, a wallet “stores the public key of the Bitcoin address and its associated private key.” (CB-1006, ¶8; CB-1007, ¶5; CB-1008, ¶5.) This public/private key pair is known as “*an asymmetric key pair.*” (See §V.B.2; CB-1003, ¶¶180, 34.) Hearn’s micropayment contract protocol (Example 7) uses the public/private key pair for Party B. Specifically, Party A “[r]equests a public key from the server.” (CB-1009, 5 (step 1).) Thus, Hearn discloses Party B has a “*public key.*” (CB-

1003, ¶¶180, 34.) Because a public key has an associated private key, a POSITA would further understand the server also has a “*private key*.” (*Id*; see also, §IV.A.2.)

Thus, the combination of Hearn and Armstrong discloses “*a second memory for storing a second asymmetric key pair, the second asymmetric key pair comprising a second private key and a second public key*” [1B.1]. (CB-1003, ¶180.)

b. “*Second Computer Processor*” actions

As discussed in §V.A.3, in the combination of Hearn and Armstrong, the component acting as Party B’s payment module (“*first client device*”) is configured to support Hearn’s micropayment contract. Therefore, this component implements Hearn’s micropayment protocol including processing the required transactions (T1, T2, and T3). (CB-1003, ¶181.) Accordingly, the combination of Hearn and Armstrong teaches or suggests the “*processor*” of the component acting as Party B’s payment module (second host computer or Party B’s user device; “*first client device*”) is configured to perform the functions recited in limitations [7B.3a]-[7B.3e] as detailed below. (*Id.*)

(i) ***“Read the Second Private Key” [7B.3a], “Read the Inchoate Data Record” [7B.3b], “Compute a Second Cryptographic Signature” [7B.3c]***

The combination of Hearn and Armstrong teaches “*read[ing] the second private key from the second memory*” [7B.3a], “*read[ing] the inchoate data record*” [7B.3b], and “*comput[ing] a second cryptographic signature from the second private key*” [7B.3c]. (CB-1003, ¶¶182-184.)

In Hearn, Party A provides the initial version of T3 (“*inchoate data record*”) to Party B. (CB-1009, 5 (step 7); CB-1003, ¶183.) As discussed in §V.B.9, the component acting as Party B’s payment module stores a copy of initial T3. During the contract, Party A “adjusts its copy of T3 to allocate more value to the server’s output and less to its ow [sic]” and sends the “signature and the amount to increment” T3 to Party B. (CB-1009, 5 (step 9).) Party B then “adjusts its copy of T3 to match the new amounts.” (*Id.*) To adjust its copy of T3, the component acting as Party B’s payment module (the second host computer or Party B’s user device) “*read[s] the inchoate data record*” [7B.3b]. (CB-1003, ¶183.)

At conclusion of the contract, Party B “**signs** and broadcasts the last transaction” (i.e., the final version of T3). (CB-1009, 5; CB-1003, ¶184.) The digital signature is created using Party B’s private key. (CB-1003, ¶184; *see also*, §IV.A.2) Accordingly, Hearn teaches use of a “*private key*” to “*compute a first cryptographic signature*” [7B.3c]. (CB-1003, ¶184.)

The “*memory*” of the “*first client device*” stores the “*private key*” and “*public key*” associated with Party B. (See §VI.B.3.a.) A POSITA would have therefore understood the “*second private key*” of Party B must be “*read*” [7B.3a] from “*the second memory*” to compute the second cryptographic signature for the final version of transaction T3. (CB-1003, ¶185.)

(ii) “*Create a Complete Data Record*” [7B.3d]

Petitioner established in §V.B.8 “*the inchoate data record is used by ... the first client device ... to create a complete data record.*” For the reasons set forth in §V.B.8, the “*second computer processor*” of the “*the first client device*” “*create[s] a complete data record*” [7B.3d]. (CB-1003, ¶¶186-187.)

The final version of T3 (“*complete data record*”) comprises “*the commit input*” [7B.3d.i], “*the output data*” [7B.3d.ii], “*the first cryptographic signature*” [7B.3d.iii], and “*the second cryptographic signature*” [7B.3d.iv]. (CB-1003, ¶187.)

Transaction T3 “connects to T1.” (CB-1009, 5 (step 7); See §V.B.6.b.i.) That is, the output of T1 is the “*commit input*” [7B.3c.i] for all versions of transaction T3 including the final version, as shown in Miller Figure E below. (CB-1003, ¶187.) The final version of T3, like the initial version of T3, has “two outputs” — one to Party A and one to Party B. (CB-1009, 5.) When the session ends or the expiration time “is close to expiry”, Party B “signs and broadcasts the last transaction it saw, allocating the final amount to itself.” (*Id.*) That is, the

maximum amount for the contract is allocated to Party B in the final version of the T3 data record as shown below. (CB-1003, ¶187.) The “two outputs” (BTC amounts) of final T3 are “*the output data*” [7B.3c.ii]. (*Id.*) Because both parties sign the final version of T3, final T3 (“*complete data record*”) includes the “*first cryptographic signature*” [7B.3c.iii] and “*second cryptographic signature*” [7B.3c.iv]. (*Id.*)

Transaction ID (T1)

INPUTS From:

previous transaction received by client A 10 BTC

OUTPUTS To:

Output 0: Party B Address 10 BTC 2 K1 K2 2 CHECKMULTSIG

DIGITAL SIGNATURE

Transaction ID (Transaction T3 – first iteration)

INPUTS From:

Transaction T1 10 BTC ← **commit input**

OUTPUTS To:

at time t0

Output 1: K1 10 BTC

Output 2: K2 0 BTC

DIGITAL SIGNATURE (client)

at time t1

Output 1: K1 5 BTC

Output 2: K2 5 BTC

at time t2 (final)

Output 1: K1 0 BTC

Output2: K2 10 BTC

DIGITAL SIGNATURE (client – K1) ← **first cryptographic signature**

DIGITAL SIGNATURE (server – K2) ← **second cryptographic signature**

Miller, Figure E

(iii) “Create a Transaction” [7B.3e].

In §V.B.8, Petitioner established the component acting as Party B’s payment module (second host computer or Party B’s user device) “*create[s] the transaction*

by broadcasting the complete data record ... for recording in the distributed ledger” [1E]. Party B “broadcasts” the final version of T3 to the Bitcoin network for verification. (CB-1009, 5; CB-1006, ¶10; CB-1007, ¶7; CB-1008, ¶7.) Armstrong’s Bitcoin network 12 is the “*transfer mechanism.*” (See §§V.B.1, VI.B.1.)

Thus, for these reasons and the reasons discussed in §V.B.8, the combination of Hearn and Armstrong discloses the component acting as Party B’s payment module (“*first client device*”) “*create[s] a transaction by submitting the complete data record to the transfer mechanism*” [7B.3e]. (CB-1003, ¶¶188-189.)

4. “*Second Client Device*” limitations [7C]

The combination of Hearn and Armstrong discloses the “*second client device*” includes “*a third memory*” [7C.1], “*a third network interface*” [7C.2], and “*a third computer processor*” [7C.3]. (CB-1003, ¶¶190-193.)

As discussed in §V.B.1, Armstrong’s second user device is the “*second client device.*” Each device in Armstrong’s network utilizes the “computer system” architecture illustrated in Figure 74. (CB-1006, ¶225-226; CB-1007, ¶58; CB-1008, ¶93; CB-1003, ¶191.) For the reasons discussed in §VI.B.3.a and §§V.B.2-5, Armstrong’s second user device (“*the second client device*”) includes “*a third memory*” [7C.1], “*a third network interface*” [7C.2], and “*a third computer*

processor coupled to the third memory and the third network interface” [7C.3].

(CB-1003, ¶191.)

In the combination of Hearn, Armstrong, and Ziegler, the “*second user device*” generates an “RSA Public/Private Key pair.” (CB-1010, 4:47-48.) The key pair is stored in a memory at the client device. The private key is then read by the processor of the client device to perform decryption during communication and data key establishment. (CB-1010, 4:46-47; 5:10-28; *See* §VI.A.1.)

Accordingly, the combination of Hearn, Armstrong, and Ziegler teaches the “*second client device*” includes a memory for “*storing a third asymmetric key pair, the third asymmetric key pair comprising a third private key and a third public key*” [7C.1] and a processor “*configured to read the third private key from the third memory*” [7C.3]. (CB-1003, ¶¶190-193.)

5. “Sign[]” and “Save a Copy of the Inchoate Data Record” [7D]

Limitation [7D] is identical to limitation [1F]. For the reasons discussed in §V.B.9, the combination of Hearn and Armstrong discloses limitation [7D]. (CB-1003, ¶194.)

6. “Distributed Ledger” [7E]

Limitation [7E] is substantially identical to limitation [1D]. The primary difference is that [1D] recites “*the decentralized digital currency comprises a distributed ledger*” whereas [7E] recites “*the transfer mechanism comprising a*

decentralized digital currency that comprises a distributed ledger.” As discussed in §V.B.1, “*the transfer mechanism compris[es] a decentralized digital currency.*” Accordingly, for the reasons discussed in §§V.B.1, V.B.7, the combination of Hearn and Armstrong discloses limitation [7E]. (CB-1003, ¶195.)

7. “*Transaction is Created by Broadcasting*” [7F]

Limitation [7F] is substantially identical to a portion of [1E] (“*creat[ing] the transaction by broadcasting the complete data record for transmitting and receiving among network participants in the computer network¹² for recording in the distributed ledger*”). For the reasons discussed in §V.B.8, the combination of Hearn and Armstrong also discloses limitation [7F]. (CB-1003, ¶196.)

8. “*Verif[y] the Recording of the Complete Data Record in the Distributed Ledger*” [7G]

Limitation [7G] is identical to limitation [1G]. For at least the reasons discussed in §V.B.10, the combination of Hearn and Armstrong discloses limitation [7G]. (CB-1003, ¶197.)

¹² “[T]he computer network” lacks antecedent basis. Solely for purposes of this Petition, Petitioner assumes the term refers to “*a computer network [associated with the transfer mechanism]*.” Petitioner reserves the right to challenge the term as indefinite in another forum.

C. Dependent Claim 8

Claim 8 recites substantially the same subject matter as claim 3 with the sole difference being claim 8 recites a “*third cryptographic signature*” because independent claim 7 recites “*first*” and “*second*” cryptographic signatures. Accordingly, for the reasons discussed in §V.D, the combination of Armstrong, Hearn, and Ziegler renders obvious claim 8. (CB-1003, ¶198.)

VII. DISCRETIONARY DENIAL IS NOT APPROPRIATE

A. 35 U.S.C. §325(d)

The prior art and arguments presented in the Petition were not previously considered by the Office. Neither Armstrong nor Ziegler was presented to the Office during prosecution. While Hearn is mentioned in the Background section of the '566 patent, Hearn was not provided by Applicant in an Information Disclosure Statement or cited separately by the Examiner. (*See* CB-1001, 3:39-46, (56).) Hearn, therefore, like Armstrong and Ziegler, was not discussed or considered by the Examiner. Importantly, none of the Petition’s grounds were considered during prosecution. The first part of the *Advanced Bionics* framework is therefore not satisfied. *Advanced Bionics, LLC v. Med-El Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6, (PTAB Feb. 13, 2020) (precedential). Moreover, the Declaration of Dr. Miller and Petitioner’s supporting extrinsic evidence were not available to the Examiner. Therefore, even if the second part of the *Advanced*

Bionics framework is considered, the evidence and facts presented in the petition warrant consideration of the Petition by the Office.

B. 35 U.S.C. §314(a)

The '566 patent was asserted against Petitioner in late September 2022 in the District of Delaware. The *Fintiv* factors weigh heavily against discretionary denial of this petition because trial occurs in the pending litigation against Petitioner after final written decision. The median-time-to-trial of all civil cases in Delaware is 33.7 months. (*See* CB-1021, 14.) Assuming that timing, the Delaware trial date is approximately July 2025, 9 months **after** the final written decision.

VIII. MANDATORY NOTICES

A. Real Parties-in-Interest

The Real-Party-in-Interest is Coinbase Global, Inc.

B. Related Matters

Veritaseum Capital, LLC has asserted the '566 Patent against Petitioner in *Veritaseum Capital, LLC v. Coinbase Global, Inc.*, Civ. No. 1:22-cv-01253 (D. Del.). According to the Complaint in that litigation, “Mr. Middleton has exclusively licensed all substantial rights to his patents, including the right to sue third parties for infringement of his patents, to Veritaseum Capital, LLC.” (CB-1020, ¶6.)

Veritaseum Capital, LLC has also asserted the '566 Patent in *Veritaseum Capital, LLC v. Circle Internet Financial Ltd. et al.*, 2:22-cv-00498 (E.D.Tex.).

C. Lead and Back-Up Counsel.

Pursuant to 37 C.F.R. §§ 42.8(b)(3), 42.8(b)(4) and 42.10(a), Petitioner appoints Lori A. Gordon (Reg. No. 50,633) as its lead counsel and Dmitry Kagan (Reg. No. 74,806) as its backup counsel both at the address of Perkins Coie, LLP, Washington, D.C. 20005.

Petitioner consents to electronic service by email at the email addresses: gordon-ptab@perkinscoie.com, and kagan-ptab@perkinscoie.com.

IX. CONCLUSION

For the grounds specified above, *Inter Partes* Review of the challenged claims is respectfully requested.

Respectfully submitted,

/Lori A. Gordon/

Lori A. Gordon
Reg. No. 50,633

PERKINS COIE LLP

March 31, 2023

CLAIM APPENDIX

[1P] *A computing device for processing a transaction between a first client device, and a second client device via a transfer mechanism, the transfer mechanism comprising a decentralized digital currency, the computing device comprising:*

[1A] *a memory for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key;*

[1B] *a network interface for receiving terms, the terms comprising:*

[1B.1] *at least one of a first principal data or a second principal data;*

[1B.2] *a reference to at least one of a first data source or a second data source; and*

[1B.3] *an expiration timestamp;*

[1C] *a computer processor coupled to the memory and the network interface, the computer processor configured to:*

[1C.1] *read the first private key from the memory;*

[1C.2] *compute a first cryptographic signature from the first private key;*

[1C.3] *create an inchoate data record comprising:*

[1C.3a] *a commit input for receiving a commit data from a commit transaction;*

[1C.3b] *one or more output data obtained from at least one of the first principal data or the second principal data, and a value data from at least one of the first data source or the second data source; and*

[1C.3c] *the first cryptographic signature; and*

[1C.4] *publish the inchoate data record to at least one of the first client device or the second client device,*

[1D] *wherein the decentralized digital currency comprises a distributed ledger that enables processing the transaction between the first client device and the second client device without the need for a trusted central authority,*

[1E] *wherein the inchoate data record is used by at least one of the first client device or the second client device to create a complete data record and to create the transaction by broadcasting the complete data record for transmitting and receiving among network participants in the computer network for recording in the distributed ledger,*

[1F] *wherein at least one of the first client device or the second client device signs the inchoate data record and saves a copy of the inchoate data record on at least one of the first client device or the second client device; and*

[1G] *wherein the at least one of the computing device, the first client device, or the second client device verifies the recording of the complete data record in the distributed ledger by observing an external state.*

[7P] *A system for processing a transaction between a first client device and a second client device via a transfer mechanism, the system comprising a computing device, the first client device, the second client device, and the transfer mechanism;*

[7A] *the computing device comprising:*

[7A.1] *a first memory comprising [sic] for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key;*

[7A.2] *a first network interface for receiving terms, the terms comprising:*

[7A.2a] *at least one of a first principal data or a second principal data*

[7A.2b] *a reference to at least one of a first data source or a second data source; and*

[7A.2c] *an expiration timestamp; and*

[7A.3] *a first computer processor coupled to the first memory and the first network interface, the first computer processor configured to:*

[7A.3a] *read the first private key from the first memory;*

[7A.3b] *compute a first cryptographic signature from the first private key;*

[7A.3c] *create an inchoate data record comprising:*

[7A.3c.i] *a commit input for receiving a commit data from a commit transaction;*

[7A.3c.ii] *one or more outputs obtained from at least one of the first principal data or the second principal data, and a value data*

*from at least one of the first data source or the second data source;
and*

[7A.3c.ii] *the first cryptographic signature; and*

[7A.3d] *publish the inchoate data record to at least one of the first client device or the second client device;*

[7B] *the first client device comprising:*

[7B.1] *a second memory for storing a second asymmetric key pair, the second asymmetric key pair comprising a second private key and a second public key;*

[7B.2] *a second network interface; and,*

[7B.3] *a second computer processor coupled to the second memory and the second network interface, the second computer processor configured to:*

[7B.3a] *read the second private key from the second memory;*

[7B.3b] *read the inchoate data record;*

[7B.3c] *compute a second cryptographic signature from the second private key;*

[7B.3d] *create a complete data record comprising:*

[7B.3d.i] *the commit input;*

[7B.3d.ii] *the output data;*

[7B.3d.iii] *the first cryptographic signature; and*

[7B.3d.iv] *the second cryptographic signature; and*

[7B.3e] *create a transaction by submitting the complete data record to the transfer mechanism;*

[7C] *the second client device comprising:*

[7C.1] *a third memory for storing a third asymmetric key pair, the third asymmetric key pair comprising a third private key and a third public key;*

[7C.2] *a third network interface; and,*

[7C.3] *a third computer processor coupled to the third memory and the third network interface, the third computer processor configured to read the third private key from the third memory; and*

[7D] *wherein the at least one of the first client device or the second client device signs the inchoate data record and saves a copy of the inchoate data record on at least one of the first client device or the second client device,*

[7E] *wherein the transfer mechanism comprising a decentralized digital currency that comprises a distributed ledger that enables processing the transaction between the first client device and the second client device without the need for a trusted central authority,*

[7F] *wherein the transaction is created by broadcasting the complete data record for transmitting and receiving among network participants in the computer network for recording in the distributed ledger, and*

[7G] *wherein at least one of the computer device, the first client device, or the second client device verifies the recording of the complete data record in the distributed ledger by observing an external state*

CERTIFICATE OF WORD COUNT UNDER 37 CFR §42.24(d)

Under 37 C.F.R. §42.24(d), the undersigned certifies that the word count for this *Petition for Inter Partes Review* totals 13,937, excluding the parts exempted by 37 C.F.R. §42.24(a).

The word count was made using the built-in word count function in the Microsoft® Word software used to prepare this document.

Respectfully submitted,

/Lori A. Gordon/

Lori A. Gordon
Registration No. 50,633

Attorney for Petitioner

Date: March 31, 2023

CERTIFICATE OF SERVICE

The undersigned hereby certifies, in accordance with 37 C.F.R. § 42.205, that the foregoing **PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT 11,196,566**, Power of Attorney, and all supporting exhibits were served via overnight mail on March 31, 2023 in their entirety on the Patent Owner as detailed below:

BRUNDIDGE & STANGER, P.C.
1925 BALLENGER AVENUE, STE. 560
ALEXANDRIA, VA 22314

And served via electronic mail:

FERRY JOSEPH, PA
Rick S. Miller
rmiller@ferryjoseph.com
Moore E. David
david.moore@brundidge-stanger.com

Respectfully submitted,

/Lori A. Gordon/

Lori A. Gordon
Registration No. 50,633

Attorney for Petitioner

Date: March 31, 2023