

Copyright on the Blockchain:

SPOOL Protocol

Specification and Reference Application

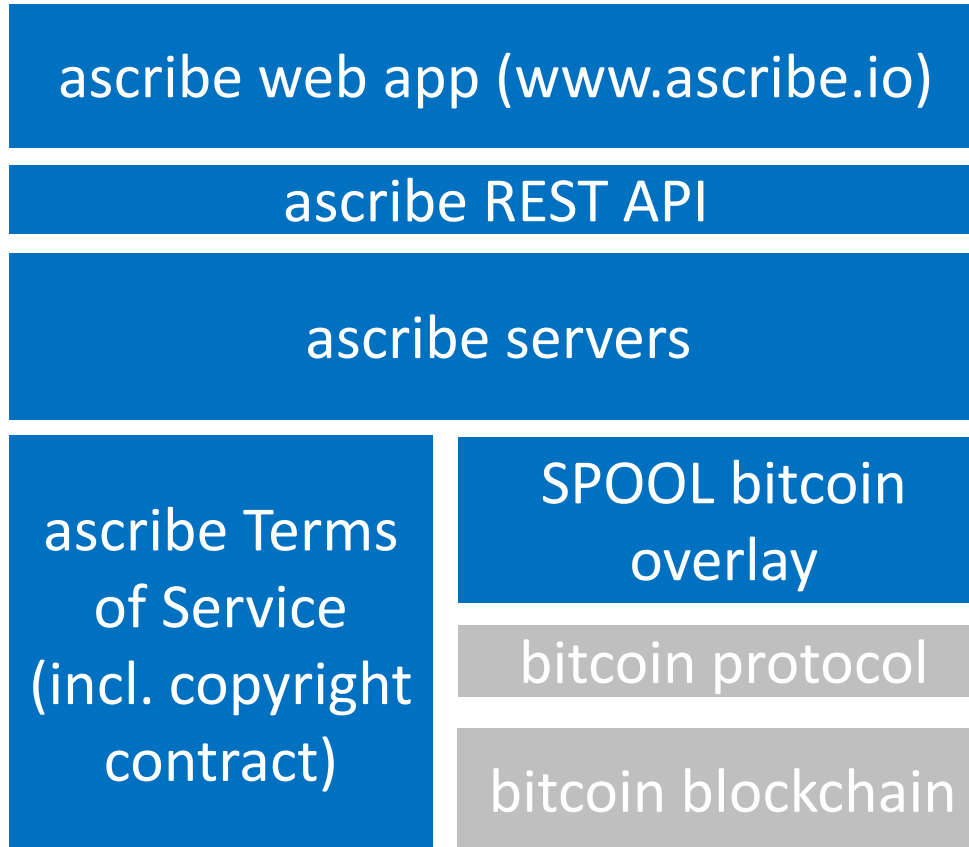
Trent McConaghy
Founder & CTO, ascribe GmbH
April 5, 2015

About SPOOL

- SPOOL is
 - a protocol for documenting transactions relating to ownership of digital property, i.e. copyright rights
 - an overlay of the bitcoin blockchain
 - SPOOL = Secure Public Online Ownership Ledger
- SPOOL is not
 - The law. SPOOL must be used with a contract concerning transfer of copyright rights that participants have agreed to. E.g. the ascribe Terms of Service (TOS).
- SPOOL transactions include
 - Register ownership. Supports >1 *unique* editions, e.g. edition 1/10, 2/10, ..., 10/10.
 - Transfer ownership
 - Consign, for someone else to sell on your behalf
 - And more
- **SPOOL + TOS = copyright on the blockchain**

Context for SPOOL

ascribe tech stack as reference implementation



SPOOL

github.com/ascribe/spool

REGISTER:

- MAPPING: 1-to-many
- SPOOL: piece_hash -> edition(s)
- BTC:

TX = [(1|tt... : 20000+num_editions)] ->
(OP_RETURN=SPOOLREGISTER:0),
> balance of piece_hash = 10000 satoshi
> balance of edition(s) = 1 satoshi

TRANSFER:

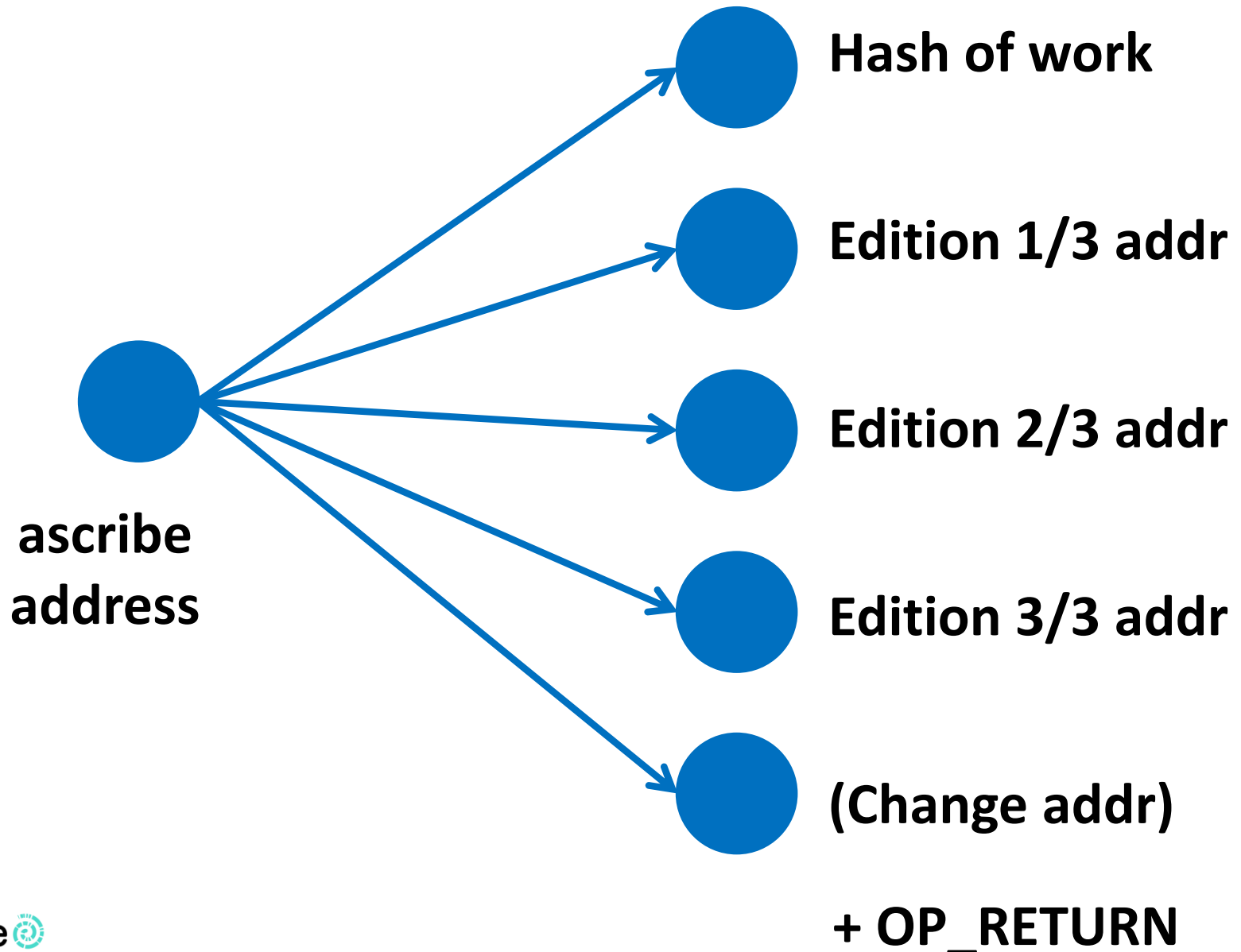
- MAPPING: 1-to-1
- SPOOL: edition -> transfered_edition
- BTC:

* first transfer
> balance of edition = 1 satoshi
TX = [(1|tt...:29999)] -> [(edition_hash:1
TX = [(edition_hash:20000)] -> transfer

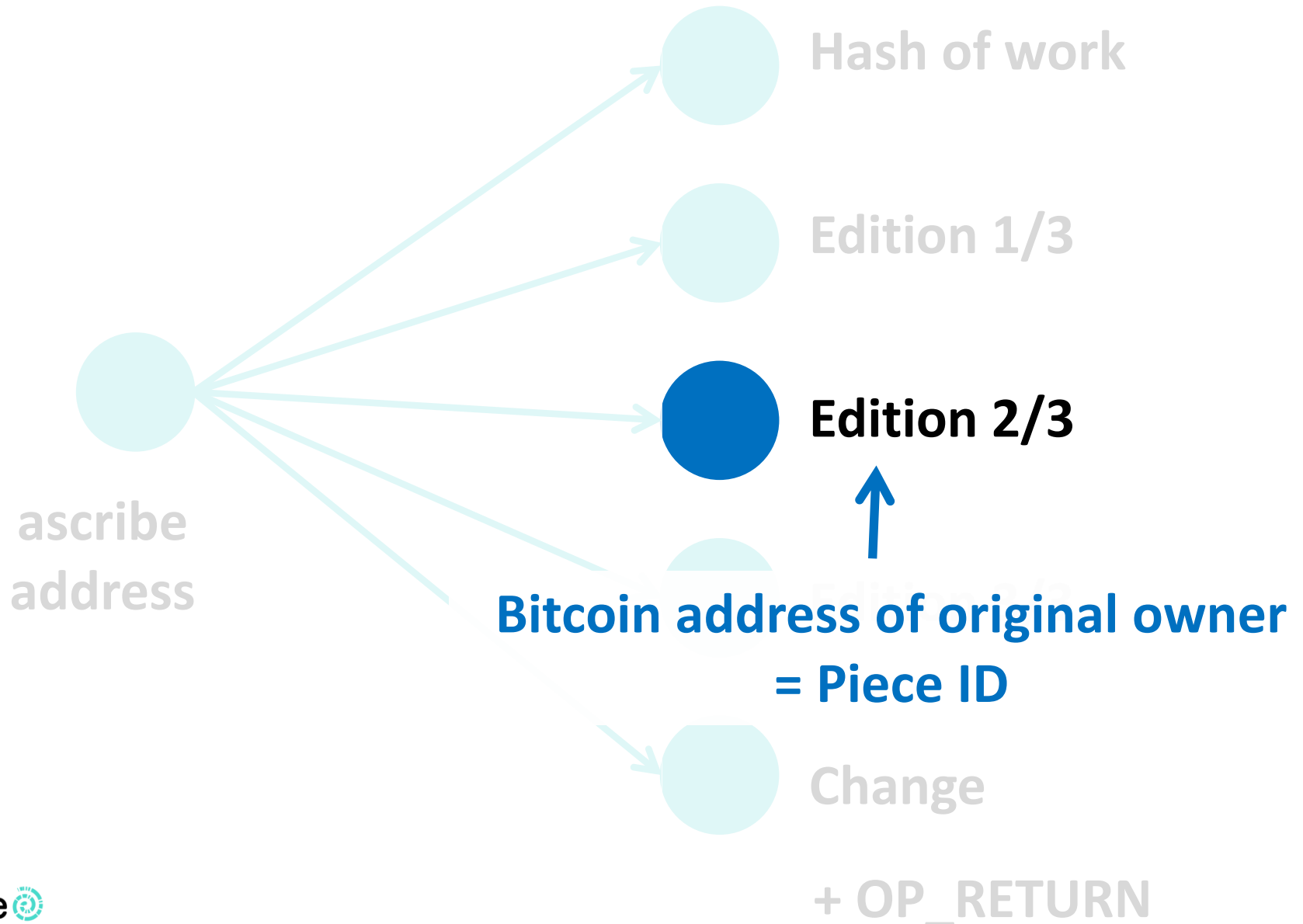
SPOOL specification

“Register” tx

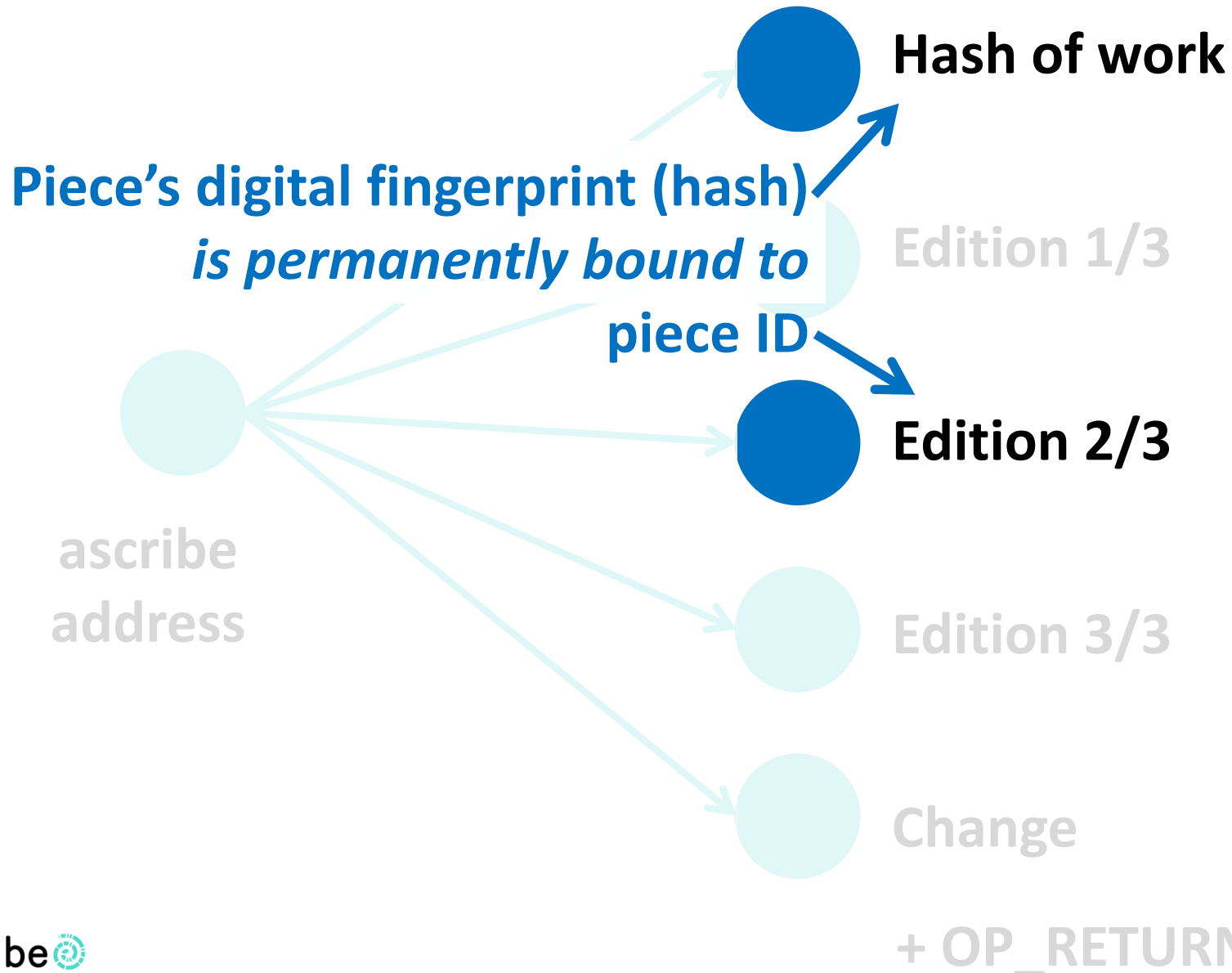
Example on 3 editions



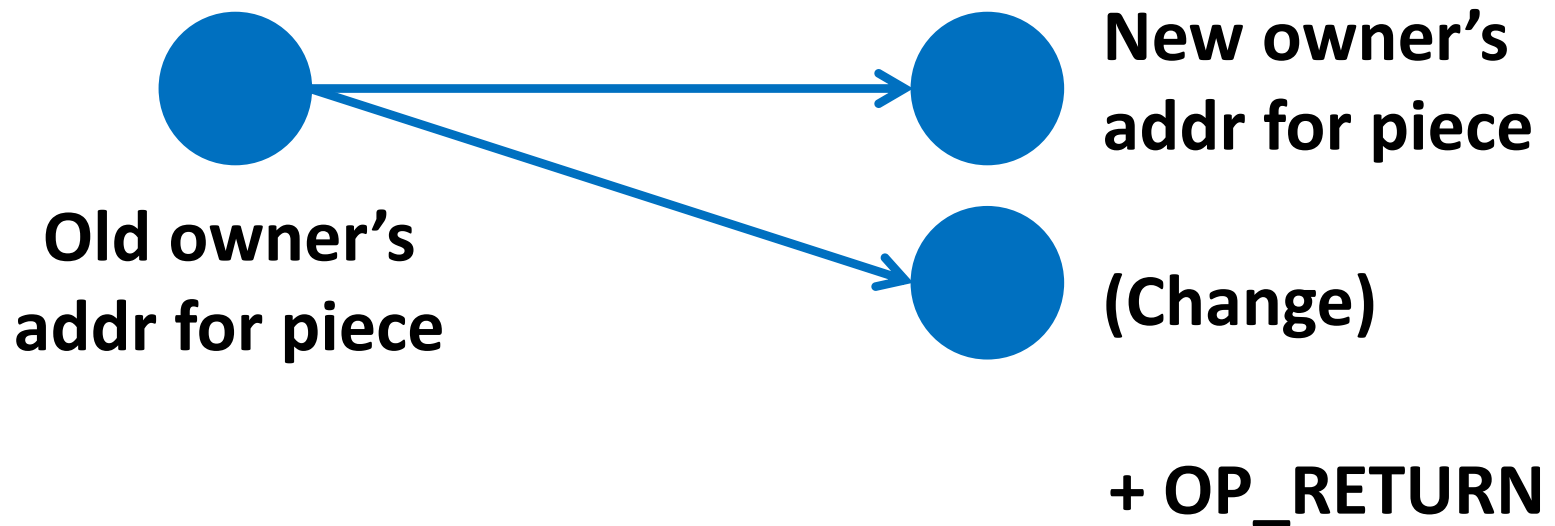
“Register” tx



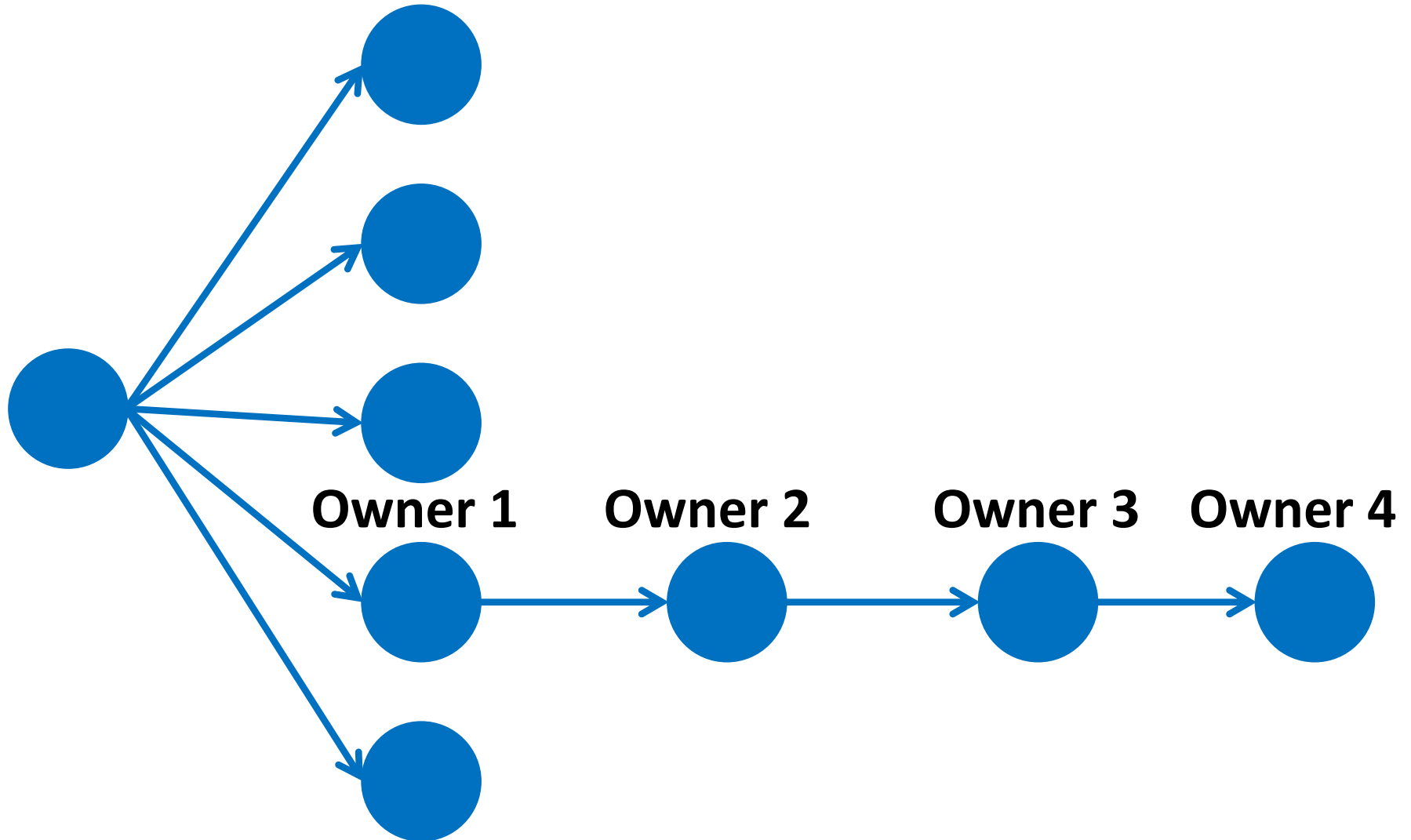
“Register” tx



“Transfer ownership” tx



Provenance (ownership history) emerges naturally



SPOOL spec

Full spec at github.com/ascribe/spool

REGISTER:

- MAPPING: 1-to-many

- SPOOL: piece_hash -> edition(s)

- BTC:

TX = [(1jtt... : 20000+num_editions)] -> [(piece_hash:10000), (edition1_hash:1), ..., (editionx_hash:1), (OP_RETURN=SPOOLREGISTER:0), (fee:10000)]

> *balance of piece_hash = 10000 satoshi*

> *balance of edition(s) = 1 satoshi*

TRANSFER:

- MAPPING: 1-to-1

- SPOOL: edition -> transfered_edition [transfered_edition is on a HD wallet owned by the transferee]

- BTC:

* first transfer

> *balance of edition = 1 satoshi*

TX = [(1jtt...:29999)] -> [(edition_hash:19999), (OP_RETURN=SPOOLREPLENISH:0), (fee:10000)]

TX = [(edition_hash:20000)] -> transfered_edition_hash [(transfered_edition_hash:10000), (OP_RETURN=SPOOLTRANSFER:0), (fee:1000)]

> *balance of edition = 0 satoshi*

> *balance of transfered_edition = 10000 satoshi*

* next transfers

> *balance of transfered_edition = 10000 satoshi*

TX = [(1jtt...:20000)] -> [(10000), (OP_RETURN=SPOOLREPLENISH:0), (fee:10000)]

TX = [(transfered_edition_hash:20000)] -> [(transfered_edition_next_hash:10000), (OP_RETURN=SPOOLTRANSFER:0), (fee:1000)]

> *balance of transfered_edition = 0 satoshi*

> *balance of transfered_edition_next = 10000 satoshi*

CONSIGN:

- MAPPING: 1-to many

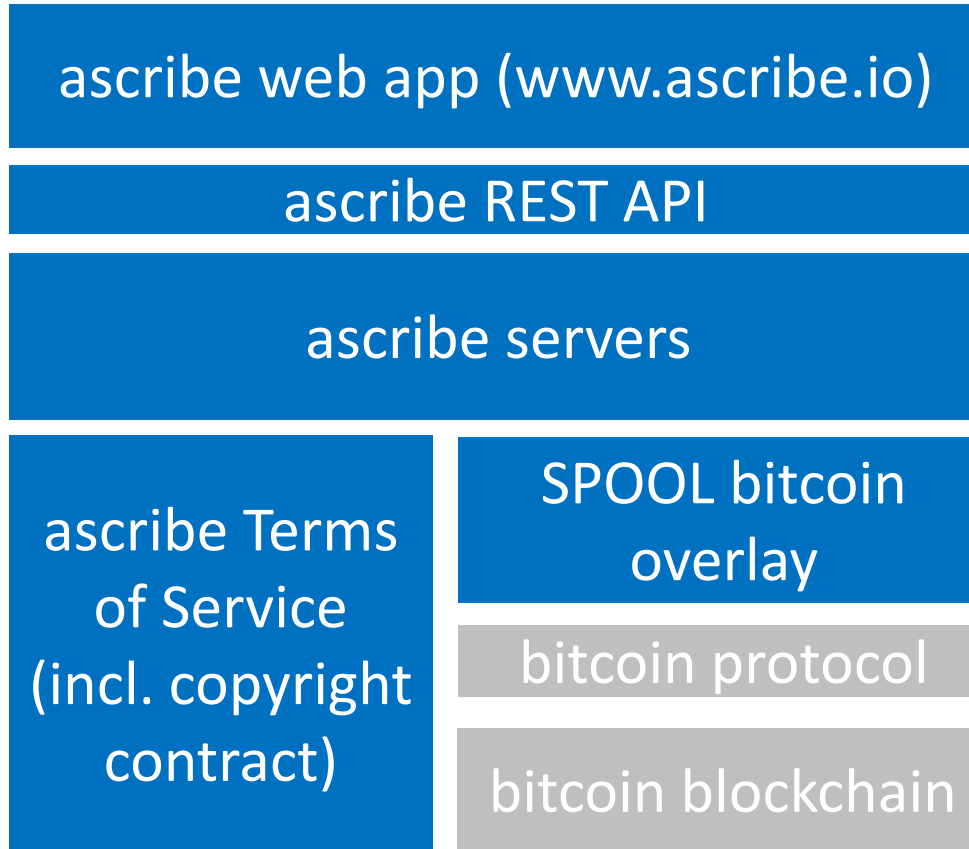
- SPOOL: edition -> consigned_edition(s) [consigned_editionx is on a HD wallet owned by consignee x]

Reference application: ascribe web app

A service for creators to register, archive, and
transfer ownership of their works

<http://www.ascribe.io>

ascribe web app in tech stack



Web app

The screenshot shows the registration form for the ascribe web app. It includes a header with the text "btc.png 15.1kB" and a "DELETE" button. Below this is a section titled "Step one: lock down title" with four input fields: "Artist's Name", "Artwork Title", "Year Created", and "Number of Editions". A note states: "This input is final and cannot be edited later. Additional details can be added after registration." At the bottom are two buttons: "REGISTER" and "CANCEL".

Welcome to ascribe!

Click or drop artwork

Step one: lock down title

Artist's Name

Artwork Title

Year Created



Number of Editions

[About / Impressum](#)

Welcome to ascribe!



btc.png 15.1kB

DELETE

Step one: lock down title

Trent McConaghy|

Bitcoin Love

2015



3

This input is final and cannot be edited later.
Additional details can be added after registration.

REGISTER

CANCEL

[About / Impressum](#)

Welcome to ascribe!



btc.png 15.1kB

DELETE

Step one: look down title

Trent McConaghy

Bitcoin Love

2015

3

This input is final and cannot be edited later.
Additional details can be added after registration.

REGISTER

CANCEL

CONSIGN

TRANSFER



Piece detail

Trent McConaghy

BITCOIN LOVE

2015, edition: 1/3

ID: 16XcLp6mEuujWng6w6LqPNprRYbj9eUcT4

Status: Can Transfer/Consign

Owner: iheartbtc@mailinator.com

Certificate of Authenticity

CREATE

Personal Note [Show/Hide](#)

Provenance/Ownership History [Show/Hide](#)

Consignment [Show/Hide](#)

Further Details [Show/Hide](#)

+ Add Display instructions

+ Add Technology details

+ Add Artist contact info


+ Add Optional data files

SPOOL Details [Show/Hide](#)

Delete Actions [Show/Hide](#)



All works =archive =wallet

ascribe 

iheartbtc@mailinator.com 

+ ARTWORK



Artist

▼ Title

Edition

Action



Trent McConaghy

Bitcoin Love

ID: 16XcLp6mEuujWng6w6LqPNprRYbj9eU...

2015, 1/3

Can Transfer/Consign



Trent McConaghy

Bitcoin Love

ID: 16fv1VhXK2gVE1hpgxpBfzdDxEa7M...

2015, 2/3

Can Transfer/Consign



Trent McConaghy

Bitcoin Love

ID: 1LPjuoXom5B5E6DQkj7Pux4QLBiWZXi...

2015, 3/3

Can Transfer/Consign

[About / Impressum](#)

CONSIGN

TRANSFER



Transfer artwork



Transferee email

Hi,

I transfer ownership of "Bitcoin Love" to you.

Truly yours,
iheartbtc@mailinator.com

Make sure that display instructions and technology details are correct.
They cannot be edited after the transfer.

Password

TRANSFER

CLOSE

Transfer ownership

CREATE

Show/Hide

+ Add Technology details

+ Add Artist contact info

+ Add Optional data files

SPOOL Details Show/Hide

Artwork ID: 16XcLp6mEuujWng6w6LqPNprRYbj9eUcT4 [Blockchain] [Raw]

Hash of artwork, title, etc: 13ewcT3FxfmiNAaNcpMyiRqkr3TK9nYq61 [Blockchain] [Raw]

Owned by SPOOL address: 16XcLp6mEuujWng6w6LqPNprRYbj9eUcT4 [Blockchain] [Raw]

Interesting aside:

While this is a *bitcoin* app,
you don't have to know bitcoin at all.
Though if you do, you can cross-check...

Further Details [Show/Hide](#)

+ Add Display instructions

+ Add Technology details

+ Add Artist contact info

+ Add Optional data files

SPOOL Details [Show/Hide](#)

Artwork ID: 16XcLp6mEuujWng6w6LqPNprRYbj9eUcT4 [\[Blockchain\]](#) [\[Raw\]](#)

Hash of artwork, title, etc: 13ewcT3FxfmiNAaNcpMyiRqkr3TK9nYq61 [\[Blockchain\]](#) [\[Raw\]](#)

Owned by SPOOL address: 16XcLp6mEuujWng6w6LqPNprRYbj9eUcT4 [\[Blockchain\]](#) [\[Raw\]](#)

**Easily cross-ref
blockchain 1/3**

Easily cross-ref blockchain 2/3

<https://blockchain.info/tx/c451dd9f6984c9870d925ca88067114dbc0bc4d8c843f96503b94eafd4a5fad4>



[Home](#) [Charts](#) [Stats](#) [Markets](#) [API](#) [Wallet](#)

Search



Transaction View information about a bitcoin transaction

c451dd9f6984c9870d925ca88067114dbc0bc4d8c843f96503b94eafd4a5fad4

1JttRRdtAi6cDNM23Uq4BEU61R8kJeANJs



13ewcT3FxfmiNAaNcpMyiRqkr3TK9nYq61
16XcLp6mEuujWng6w6LqPNprRYbj9eUcT4
16fv1VhXK2gVE1hpgxpBfzdDxEnCa7MpYn
1LPjuoXom5B5E6DQkj7Pux4QLBiWZXiC7N
1JttRRdtAi6cDNM23Uq4BEU61R8kJeANJs

Unable to decode output address

0.0001 BTC
0.000006 BTC
0.000006 BTC
0.000006 BTC
0.000182 BTC
0 BTC

7 Confirmations
















0.0003 BTC

Summary

Size	359 (bytes)
Received Time	2015-03-22 13:50:30
Included In Blocks	348695 (2015-03-22 13:50:30 + 0 minutes)
Confirmations	7 Confirmations
Relayed by IP	144.76.13.207 (whois)
Visualize	View Tree Chart




Inputs and Outputs

Total Input	0.0004 BTC
Total Output	0.0003 BTC
Fees	0.0001 BTC
Estimated BTC Transacted	0 BTC
Scripts	Show scripts & coinbase

2015 12:57 GMT	6e00e07b0e	6a2606ed3162cb03e55ca0ed5e93ab88de53a70a4da37464d7179e386d706	
		9256c1318ebbc (raw)	
348843	590db4315682e4c870387b8be37	??_???M???7^?y?>?UN???az?R\$5????m???????	
23 Mar 2015 12:57 GMT	07d7318383123d98e046f0489fd ca04199718	ouhf3LT9TcsAITdeFXnDPgpVTvuhn2F67llkNcfll0lJtAAAA1hAAAA== (base64) 6a28a2e85fdc b4fd4dc b0095375e1579c 33e0a554efba19f617aee522435c 7c 8d082 6d000000d6100000 (raw)	
348838	c1ccc8398d3eaf42df3a135ed12	ASCRIBESPOOLREGISTER	
23 Mar 2015 12:29 GMT	1a1fff80832528791e8897eb257b 8a486c1cc	QVNDUKICRVNQT09MUKVHSVNUrVI= (base64) 6a144153435249424553504f4fc5245474953544552 (raw)	
348837	7b99e0d3fa9d4d24d2f02871533f	BITPROOF?kf?^U?????:????Bx?~::?????k(???r (Bitproof)	
23 Mar 2015 12:19 GMT	d4a2bf8d4d512ee5407d7d898b2 9c709d4e3	QkIUUFJPT0YCa2b+XIXp2uTgOoPE4dNCeN5+Ojrv0P7Y7Gso7lgYcg== (base64) 6a2842495450524f46026b66fe5e55e9dae4e03a83c 4e1d34278de7e3a3aefd0fed 8ec6b28ec 881872 (raw)	
348828	649e8ebf8007ae56f4a8be5c571	ASCRIBESPOOLREGISTER	
23 Mar 2015 11:03 GMT	887c2eab61828b5b0917d098a8b fcb2d15f6b	QVNDUKICRVNQT09MUKVHSVNUrVI= (base64) 6a144153435249424553504f4fc5245474953544552 (raw)	
348828	ea39fb870979b5121bc815043f2	ASCRIBESPOOLREGISTER	
23 Mar 2015 11:03 GMT	2bd455fcc4c07e88cc30e8fe5f3c 830df98a9	QVNDUKICRVNQT09MUKVHSVNUrVI= (base64) 6a144153435249424553504f4fc5245474953544552 (raw)	
348828	25292c3e7a6b90ba6116f5a06ef	ASCRIBESPOOLREGISTER	
23 Mar 2015 11:03 GMT	51d08b027e2c8d56b033da94abf 127b2fd11e	QVNDUKICRVNQT09MUKVHSVNUrVI= (base64) 6a144153435249424553504f4fc5245474953544552 (raw)	
348828	076e3f6b7a5371c8b84c432749c	OA????? (Open Assets)	
23 Mar 2015 11:03 GMT	89fc54f5e72890f7502f4e56b0f2e 634722c8	T0EBAAEKAA== (base64) 6a074f410100010a00 (raw)	
348828	3bde75f4cbf35ea30b8857c817	ASCRIBESPOOLREGISTER	
	d2aa40337c0b5f0d0b120c5224f5		

Webapp & SPOOL history

- Prototype – Nov 2013
 - E.g. <https://blockchain.info/tx/13b5828c281bb2c8a9448bd3cbebd9a592ba4a6b55ec4aad79b4625cb85e4c>
- alpha – Mar 2014
- beta – Sep 2014
- production v1 – Mar 2015
 - E.g. at coinsecrets.org

348828	649e8ebf8007ae56f4a0be5c571 887c2eab8182b5b0917d098a9b fcb2d1f9b	ASCRIBESPOOLREGISTER QVNDUKICRVNQTO9MUKVHSVNUVI= (base64) 6a144153435249424553504f4f4c5245474953544552 (raw)	
23 Mar 2015 11:03 GMT			
348828	ea38fb870970b5121bc815043f2 2bd455fcc407e88cc30e8fe9f3c 830df98a9	ASCRIBESPOOLREGISTER QVNDUKICRVNQTO9MUKVHSVNUVI= (base64) 6a144153435249424553504f4f4c5245474953544552 (raw)	
23 Mar 2015 11:03 GMT			
348828	25292c3e7a8b90ba8116f5a08af 51d08b027e2c0d58b033da94abf 127b2fd11e	ASCRIBESPOOLREGISTER QVNDUKICRVNQTO9MUKVHSVNUVI= (base64) 6a144153435249424553504f4f4c5245474953544552 (raw)	
23 Mar 2015 11:03 GMT			

Conclusion

- SPOOL + TOS is **copyright on the blockchain**
- SPOOL spec at github.com/ascribe/spool
- Webapp implementation at www.ascribe.io
- In production use now