Drivechain

Overview, Demo, Teasers

Construct 2017 – January 30th

Paul Sztorc

Agenda

1. What are sidechains? How SCs must work.
2. Design Philosophy – Specific choices made by DC.
3. Some technical details, and diagrams.
4. Screenshots of DC software.
5. Sneak Peak at Future Awesome Sidechains.

What are sidechains?

- An "**alt-chain**" is a blockchain with "alt" rules and abilities. (Different cost/benefit tradeoff.) :)
  - "**alt-coin**" = alt-chain + new ***monetary network***.
  - "**sidechain**" = alt-chain + inherits ***monetary network***.
  - (Note that *mone. networks* are *inherently adversarial*.) :(
- Imagine that you had to use a different unit of money in each store? Wouldn't that kind of defeat the entire purpose of money?
- Blockchain = ***competing*** currency, Sidechain = ***competing*** code (only!).
- Opt-in – user can choose all, none, or some new features. Privatization.
- Bitcoin will always have the best code, b/c it can copy anything out there!

How to make SCs?

- Given the extreme benefits of this tech, it might surprise you how close we’ve been to the solution this whole time.
- Conditional on an Altcoin Existing, take it and:
  - Add new Setup with zero initial coins, and no block subsidy. ✓
  - Find a way to secure the chain, without block rewards (and potentially without fees, as fees will be uncertain) – called “merged mining” and easy ✓
  - Add some “Accounting”
    - When main balance goes down, causes side balance to go up – easy ✓
    - When side balance goes down, causes main balance to go up - ???

How to make SCs?

- Given the extreme benefits of this tech, it might surprise you how close we’ve been to the solution this whole time.
- Conditional on an Altcoin Existing, take it and:
  - Add new Setup with zero initial coins, and no block subsidy. ✓
  - Find a way to secure the chain, without block rewards (and potentially without fees, as fees will be uncertain) – called “merged mining” and easy ✓
  - Add some “Accounting”
    - When main balance goes down, causes side balance to go up – easy ✓
    - When side balance goes down, causes main balance to go up - ???

The Critical Requirement: How does Bitcoin know ‘who to pay’ and ‘how much’?

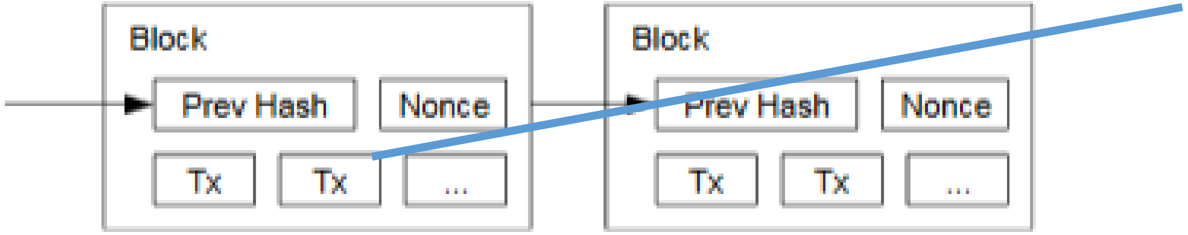
- Answer: we just assert it, blindly. Miners get to ‘pay anyone’ ‘any amount’.
- Threat Model is:
  - What if miners assert the wrong thing?
  - Are we able to protect ourselves? Can we punish transgressor(s)?
- How does the design address this threat?
  - ‘Knowing’ → ‘Caring’ → Responding (Passively and Actively)
  - Asymmetric Effort – costly to attack, (relatively) easy to block
- Next 3 slides are boring text about this.

Knowing You’re Under Attack – Learning that the Miner has Submitted Wrongly

- We can only know by checking everything for ourselves (Positive Proof).
- But that isn’t interesting! (No efficiency gain -- effective hard fork).
- Alternatively, we can get very strong evidence against ‘wrongness’ if:
  - It is easy to sound the alarm on ‘wrongness’, easy to check the alarm…
  - …and no alarm has been sounded. (Negative Proof)
- We need a “human perception” version of HashCash: easy-to-check, but difficult-to-create.
  - Easy to check: Withdrawal-validity *condenses* to one ‘true/false’ question.
  - Difficult to create: we ask the ‘t/f’ question *infrequently* (say, once per 2 or 3 months). We constrain the system such that there is only one “true” per period.
  - Thus, the ‘alarm’ is fast to check, but “slow to require”.
  - (We make up for the inconvenience later – using Atomic Swaps, LN, SoL … “layer-3”.)

Progressing: “We Know” → “We Care”

- We’ve established that [1] the assertion is blind, but [2] we can easily discover if it is incorrect. “If it were an attack, someone would have pointed it out by now”.
- We want to improve this to “if it were *anything less than perfect*, someone would have pointed it out by now”.



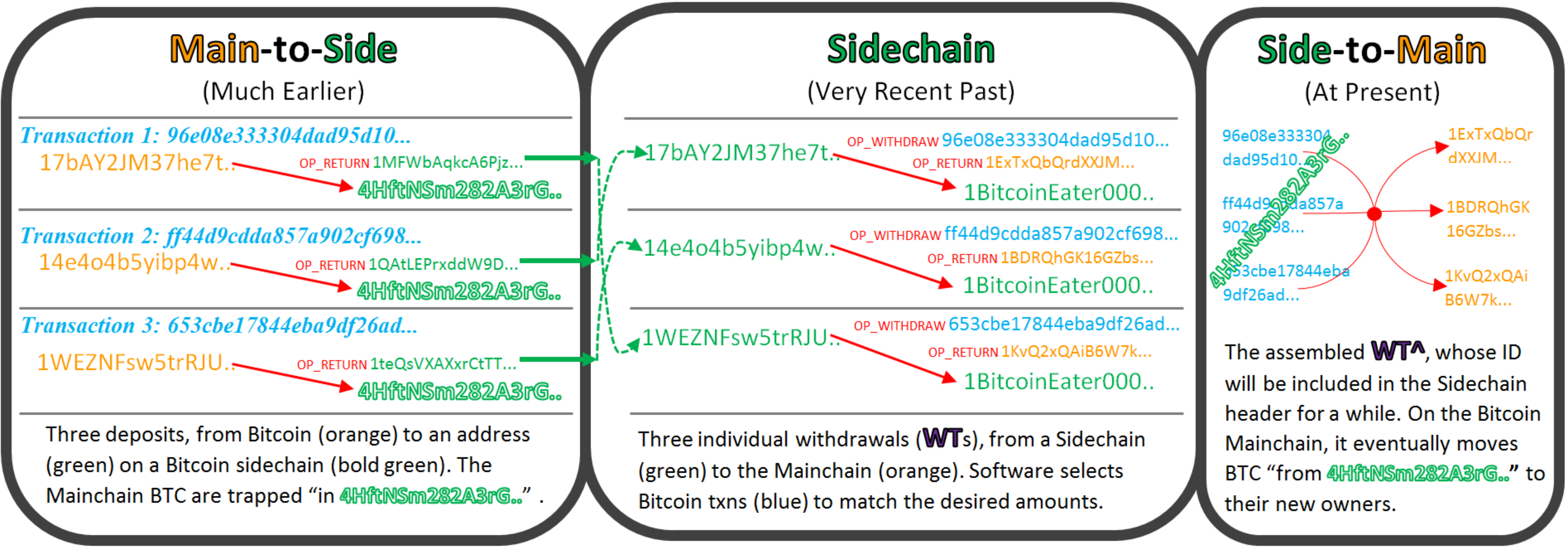
If it were possible for miner to attack *one* tx in isolation, that would be bad. Other users might say “not my problem”.
To address this, in Bitcoin, one modification screws the block up for everyone.

- Large ‘superblock’ of all withdrawal throughput.
- If the ‘true/false’ question = ‘false’, then ***no one’s funds are safe***.

Using “We Care” to inflict Penalties on Attacker

- Now, every attack will be:
  1. Obvious to everyone (easy to observe that attack is happening).
  2. Deliberate (ie, inexcusable).
  3. “Unquenchable” (miner is not demanding something reasonable – instead, asking for the ability to rob *everyone*).
- How might users react to such an attack:
  - Decline to use the sidechain (miners lose future txn fees).
  - Decline to use *any* sidechains (all txn fees lost, all SCs).
  - Adjust their valuation of BTC downward, sidechain experiment dead (this impacts the price of BTC, decreases purchasing power of Mainchain fees and even the Mainchain block subsidy).
- Call up miners, find out what’s wrong. Threaten with: new mining pools, soft fork to reject attack, HF to change PoW algo.

Details – BTC moving in and out of SC



Main-to-Side

(Much Earlier)

Transaction 1: 96e08e333304dad95d10...

17bAY2JM37he7t.. OP_RETURN 1MFWbAqkcA6Pjz...

4HftNSm282A3rG..

Transaction 2: ff44d9cdda857a902cf698...

14e4o4b5yibp4w.. OP_RETURN 1QAtLEPrxddW9D...

4HftNSm282A3rG..

Transaction 3: 653cbe17844eba9df26ad...

1WEZNFsw5trRJU.. OP_RETURN 1teQsVXAXxrCtTT...

4HftNSm282A3rG..

Three deposits, from Bitcoin (orange) to an address (green) on a Bitcoin sidechain (bold green). The Mainchain BTC are trapped "in **4HftNSm282A3rG..**" .

Sidechain

(Very Recent Past)

17bAY2JM37he7t.. OP_WITHDRAW 96e08e333304dad95d10...

OP_RETURN 1ExTxQbQrdXXJM...

1BitcoinEater000..

14e4o4b5yibp4w.. OP_WITHDRAW ff44d9cdda857a902cf698...

OP_RETURN 1BDRQhGK16GZbs...

1BitcoinEater000..

1WEZNFsw5trRJU.. OP_WITHDRAW 653cbe17844eba9df26ad...

OP_RETURN 1KvQ2xQAiB6W7k...

1BitcoinEater000..

Three individual withdrawals (**WT**s), from a Sidechain (green) to the Mainchain (orange). Software selects Bitcoin txns (blue) to match the desired amounts.

Side-to-Main

(At Present)

96e08e333304 dad95d10...

ff44d9cdda857a 902cf698...

653cbe17844eba 9df26ad...

4HftNSm282A3rG..

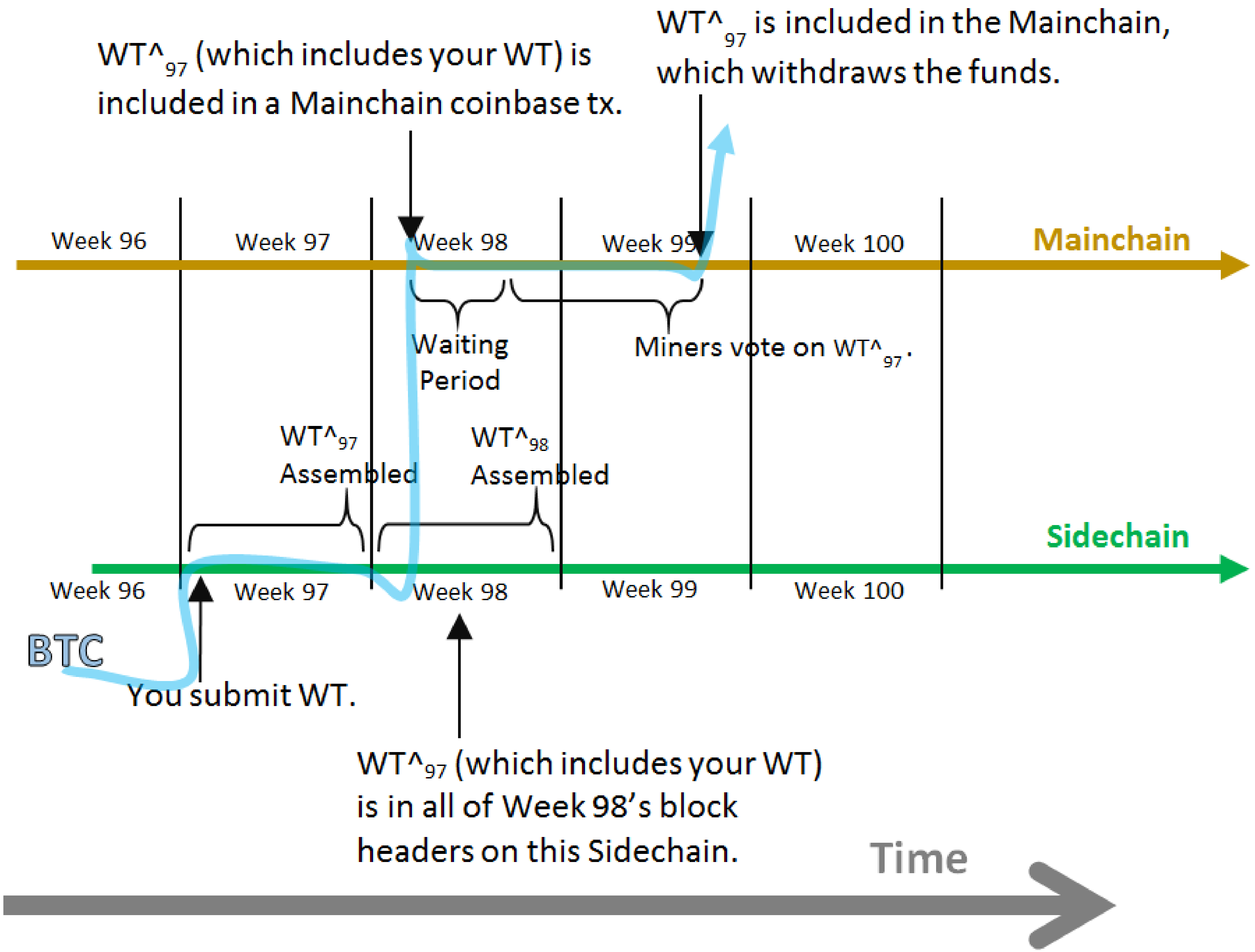
1ExTxQbQr dXXJM...

1BDRQhGK 16GZbs...

1KvQ2xQAi B6W7k...

The assembled **WT^**, whose ID will be included in the Sidechain header for a while. On the Bitcoin Mainchain, it eventually moves BTC "from **4HftNSm282A3rG..**" to their new owners.

For simplicity, I assume that all addresses/transactions contain exactly 1 BTC (except for the WT^ which contains 3 BTC).



WT^$_{97}$ (which includes your WT) is included in a Mainchain coinbase tx.

WT^$_{97}$ is included in the Mainchain, which withdraws the funds.

Waiting Period

Miners vote on WT^$_{97}$.

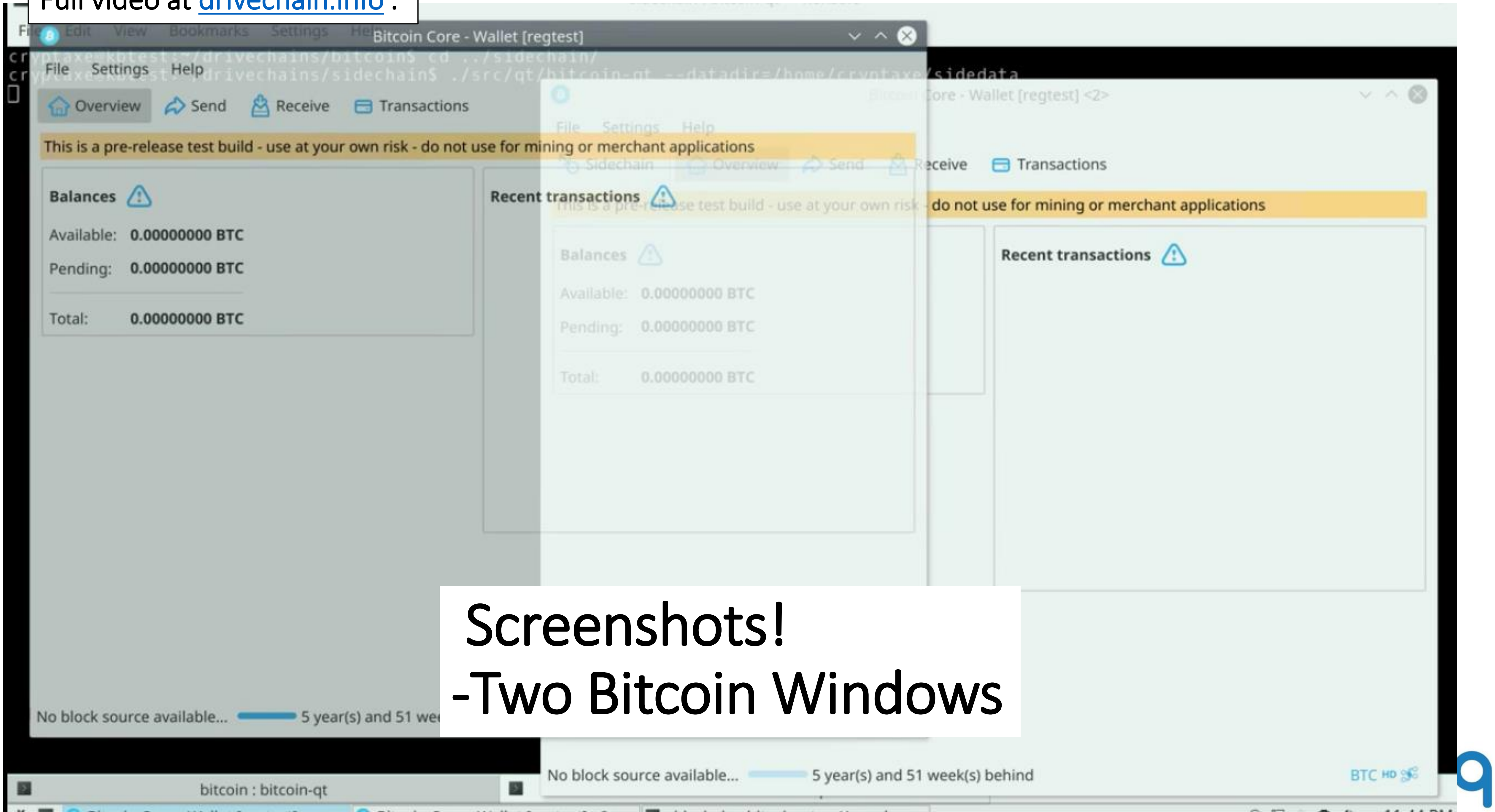
WT^$_{97}$ Assembled

WT^$_{98}$ Assembled

You submit WT.

WT^$_{97}$ (which includes your WT) is in all of Week 98's block headers on this Sidechain.

Full video at drivechain.info .



File Edit View Bookmarks Settings Help
Bitcoin Core - Wallet [regtest]
File Settings Help
Overview
Send
Receive
Transactions
Bitcoin Core - Wallet [regtest] <2>
Sidechain
bitcoin : bitcoin-qt
BTC HD

```
cryptaxe@kbtest:~/drivechains/bitcoin$ cd ../sidechain/
cryptaxe@kbtest:~/drivechains/sidechain$ ./src/qt/bitcoin-qt --datadir=/home/cryptaxe/sidedata
```

This is a pre-release test build - use at your own risk - do not use for mining or merchant applications

Balances

Available: 0.00000000 BTC

Pending: 0.00000000 BTC

Total: 0.00000000 BTC

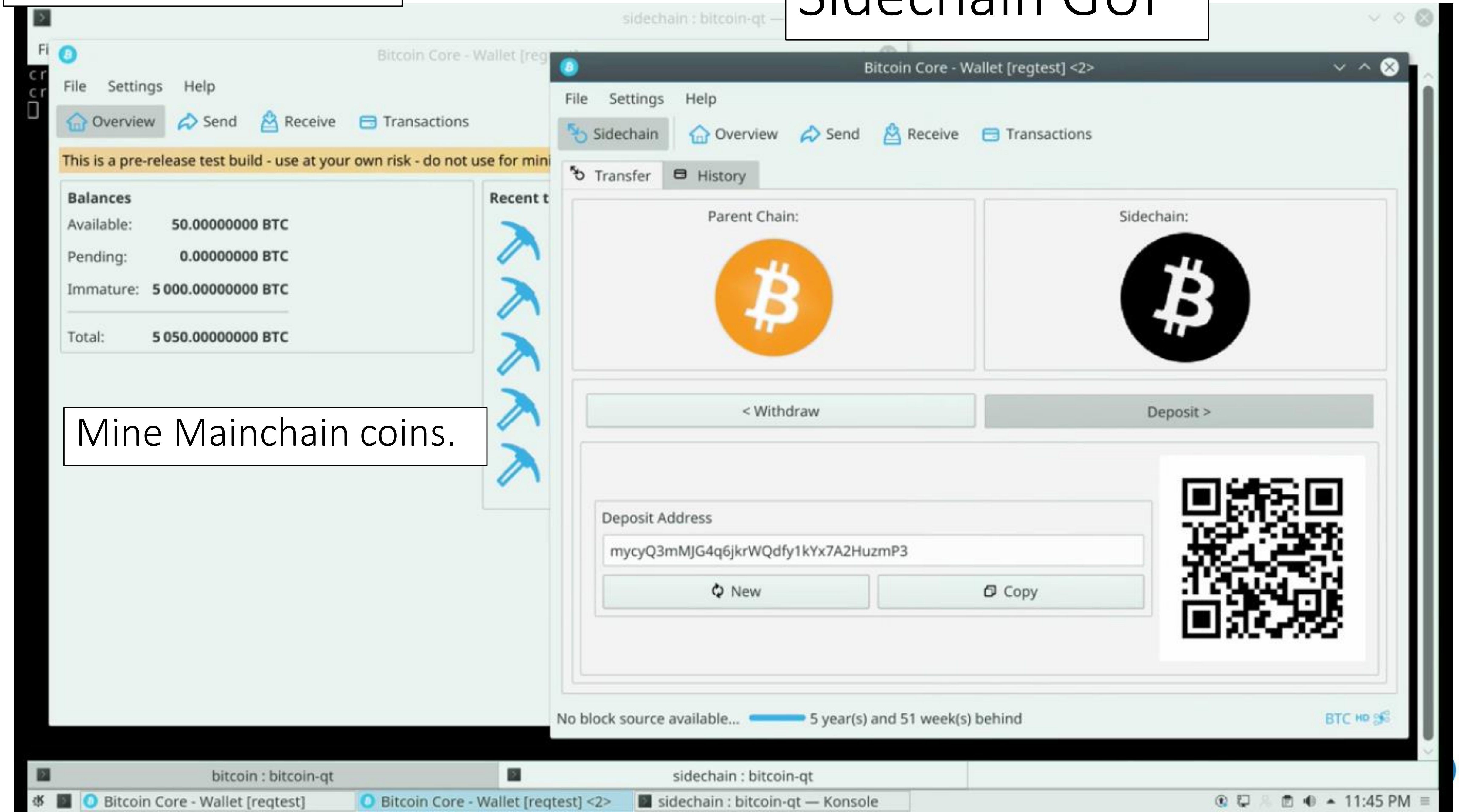
Recent transactions

No block source available... 5 year(s) and 51 week(s) behind

Screenshots!
-Two Bitcoin Windows

Full video at drivechain.info .

Sidechain GUI



Mine Mainchain coins.

Bitcoin Core - Wallet [regtest]

Balances

Available: 50.00000000 BTC

Pending: 0.00000000 BTC

Immature: 5 000.00000000 BTC

Total: 5 050.00000000 BTC

This is a pre-release test build - use at your own risk - do not use for mini

Bitcoin Core - Wallet [regtest] <2>

Parent Chain:

Sidechain:

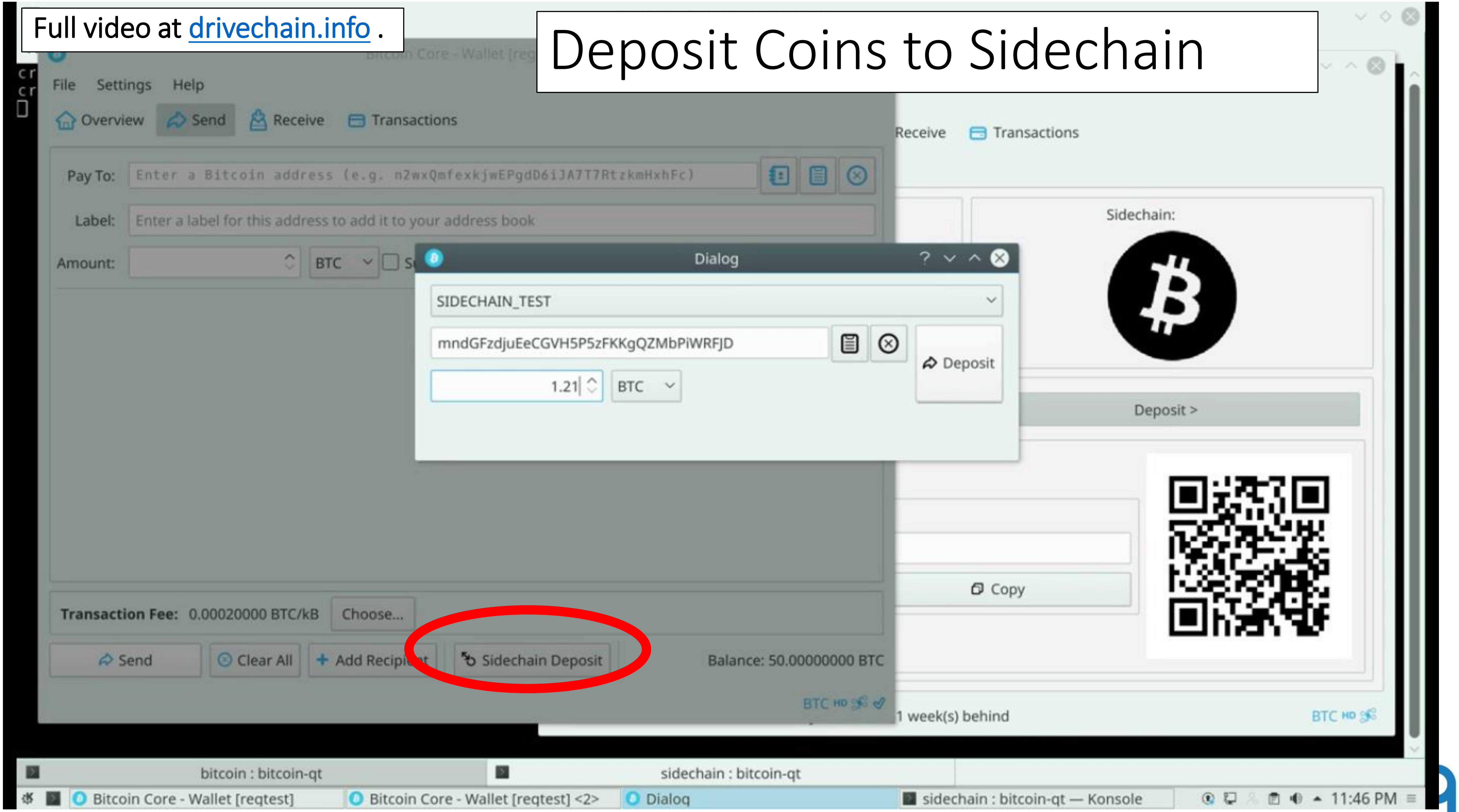
Deposit Address

mycyQ3mMJG4q6jkrWQdfy1kYx7A2HuzmP3

No block source available... 5 year(s) and 51 week(s) behind

Full video at drivechain.info .

Deposit Coins to Sidechain



Pay To: Enter a Bitcoin address (e.g. n2wxQmfexkjwEPgdD6iJA7T7RtzkmHxhFc)

Label: Enter a label for this address to add it to your address book

Amount: BTC

Dialog

SIDECHAIN_TEST

mndGFzdjuEeCGVH5P5zFKKgQZMbPiWRFJD

1.21 BTC

Transaction Fee: 0.00020000 BTC/kB

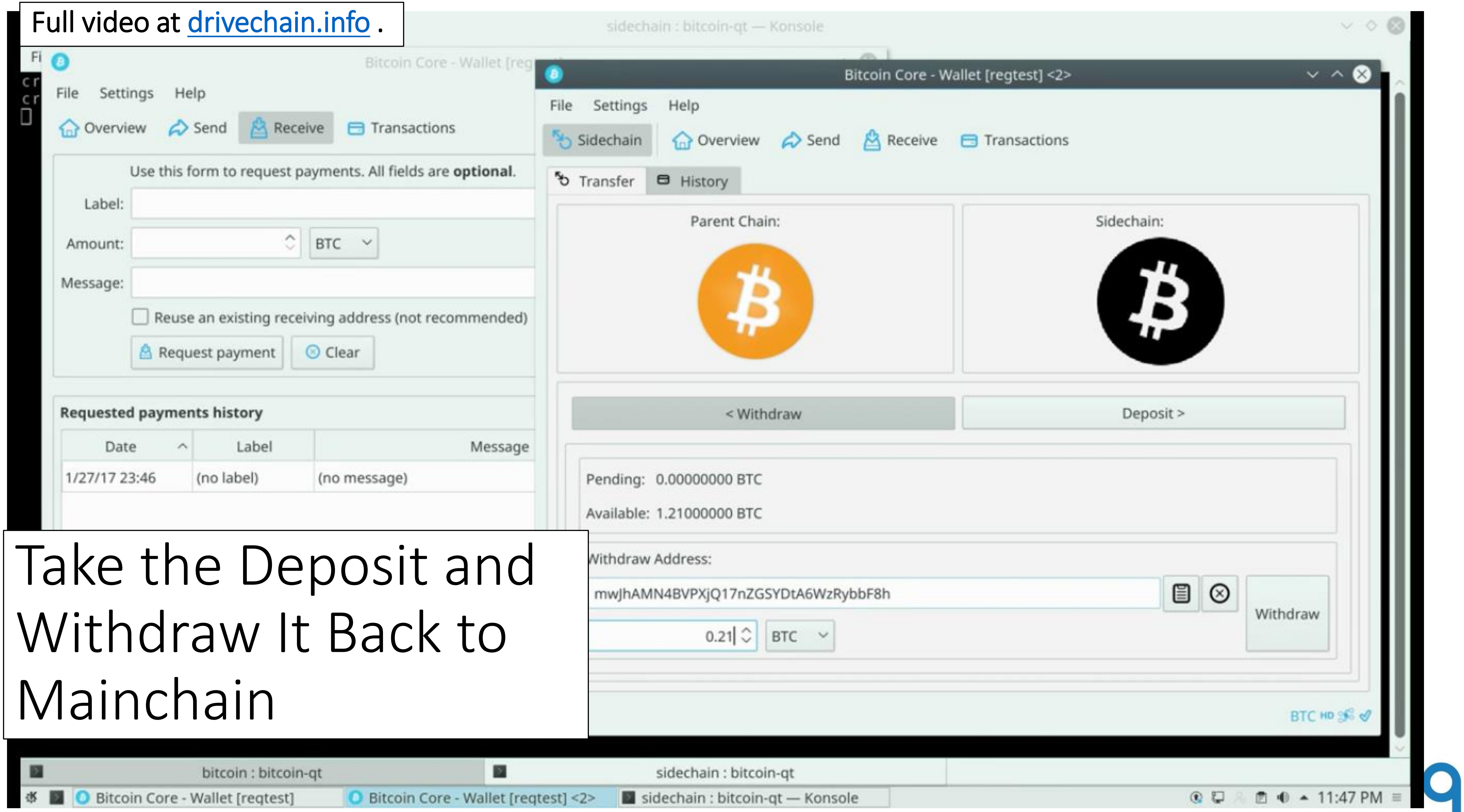
Balance: 50.00000000 BTC

Sidechain:

1 week(s) behind

Full video at drivechain.info .

Take the Deposit and Withdraw It Back to Mainchain



sidechain : bitcoin-qt — Konsole
Bitcoin Core - Wallet [regtest]
File Settings Help
Overview Send Receive Transactions

Use this form to request payments. All fields are **optional**.

Label:

Amount: BTC

Message:

□ Reuse an existing receiving address (not recommended)

Requested payments history

Date	Label	Message
1/27/17 23:46	(no label)	(no message)

Bitcoin Core - Wallet [regtest] <2>
File Settings Help
Sidechain Overview Send Receive Transactions
Transfer History
Parent Chain:
Sidechain:
< Withdraw
Deposit >

Pending: 0.00000000 BTC

Available: 1.21000000 BTC

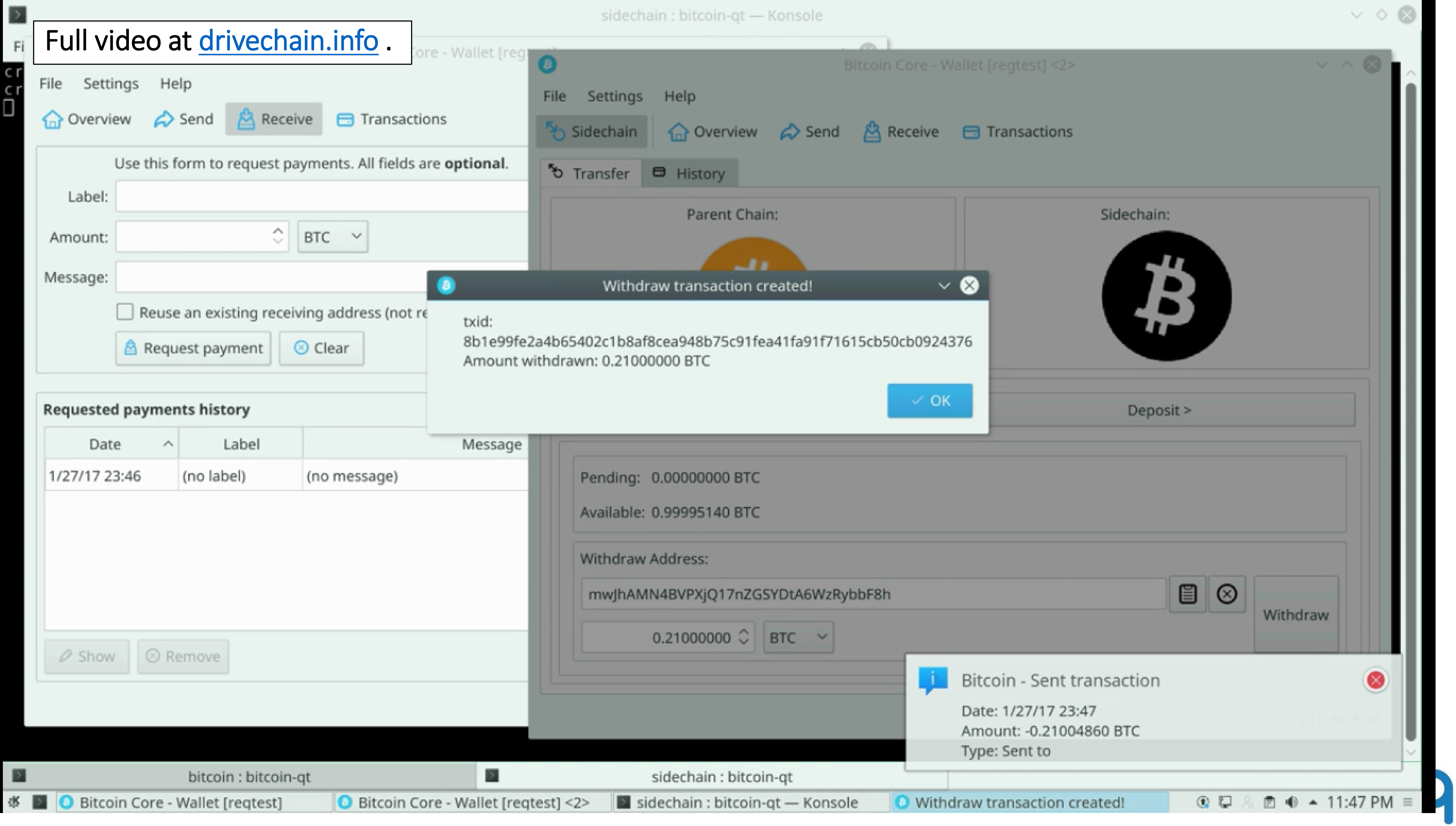
Withdraw Address:

mwJhAMN4BVPXjQ17nZGSYDtA6WzRybbF8h

0.21 BTC

Withdraw
BTC HD
bitcoin : bitcoin-qt
sidechain : bitcoin-qt
Bitcoin Core - Wallet [regtest]
Bitcoin Core - Wallet [regtest] <2>
sidechain : bitcoin-qt — Konsole
11:47 PM

Full video at drivechain.info .



Use this form to request payments. All fields are **optional**.

Label:

Amount: BTC

Message:

□ Reuse an existing receiving address (not re

Requested payments history

Date	Label	Message
1/27/17 23:46	(no label)	(no message)

Withdraw transaction created!

txid:
8b1e99fe2a4b65402c1b8af8cea948b75c91fea41fa91f71615cb50cb0924376
Amount withdrawn: 0.21000000 BTC

Pending: 0.00000000 BTC

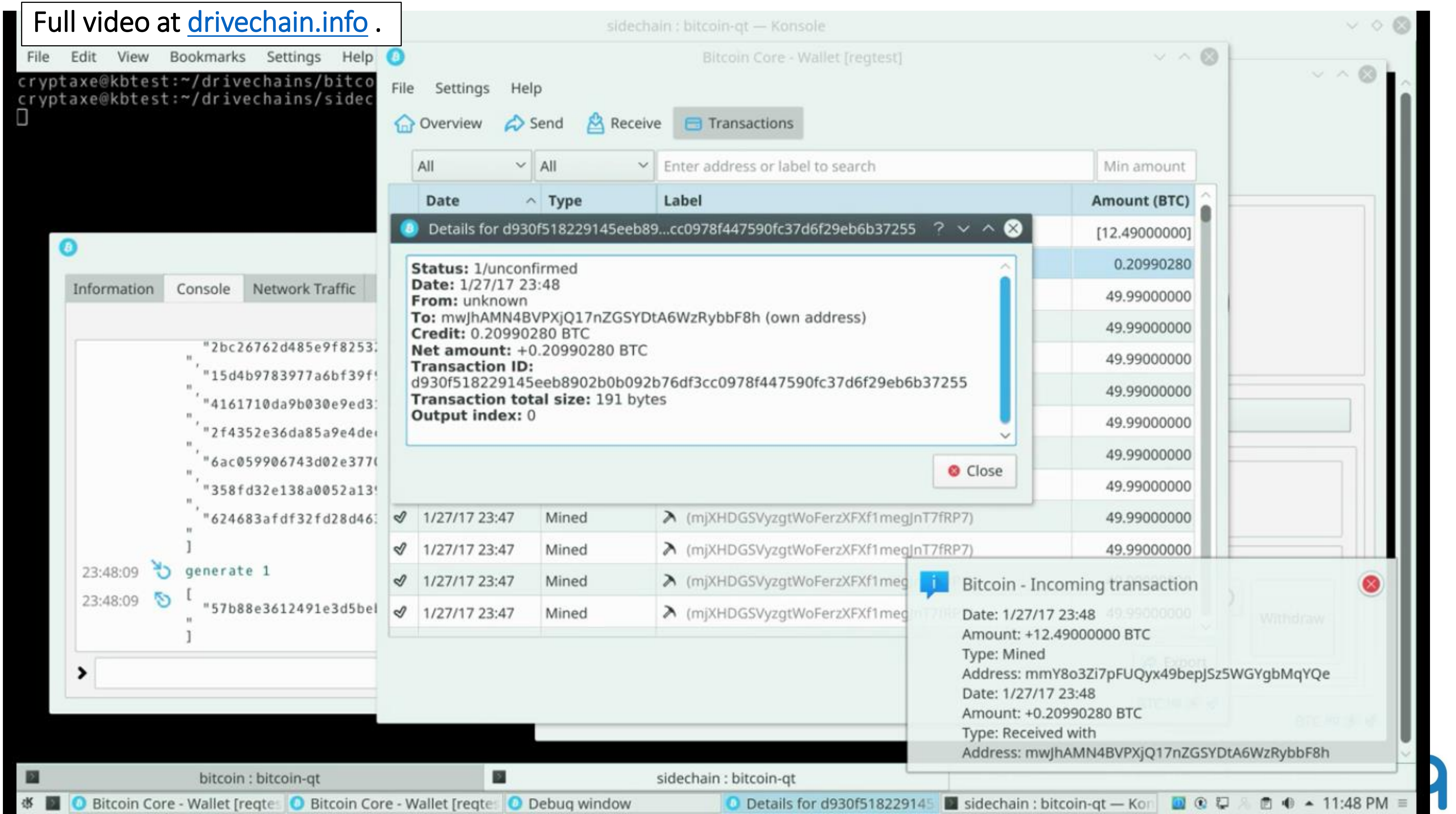
Available: 0.99995140 BTC

Withdraw Address:
mwJhAMN4BVPXjQ17nZGSYDtA6WzRybbF8h

0.21000000 BTC

Bitcoin - Sent transaction
Date: 1/27/17 23:47
Amount: -0.21004860 BTC
Type: Sent to

Full video at drivechain.info .



sidechain : bitcoin-qt — Konsole

```
cryptaxe@kbtest:~/drivechains/bitco
cryptaxe@kbtest:~/drivechains/sidec
```

Bitcoin Core - Wallet [regtest]

File Settings Help
Overview Send Receive Transactions
All All
Enter address or label to search
Min amount

Date	Type	Label	Amount (BTC)
			[12.49000000]
			0.20990280
			49.99000000
			49.99000000
			49.99000000
			49.99000000
			49.99000000
			49.99000000
			49.99000000
1/27/17 23:47	Mined	(mjXHDGSVyzgtWoFerzXFXf1megJnT7fRP7)	49.99000000
1/27/17 23:47	Mined	(mjXHDGSVyzgtWoFerzXFXf1megJnT7fRP7)	49.99000000
1/27/17 23:47	Mined	(mjXHDGSVyzgtWoFerzXFXf1meg	
1/27/17 23:47	Mined	(mjXHDGSVyzgtWoFerzXFXf1meg	

Details for d930f518229145eeb89...cc0978f447590fc37d6f29eb6b37255

Status: 1/unconfirmed
Date: 1/27/17 23:48
From: unknown
To: mwJhAMN4BVPXjQ17nZGSYDtA6WzRybbF8h (own address)
Credit: 0.20990280 BTC
Net amount: +0.20990280 BTC
Transaction ID:
d930f518229145eeb8902b0b092b76df3cc0978f447590fc37d6f29eb6b37255
Transaction total size: 191 bytes
Output index: 0

```
    "2bc26762d485e9f8253
  ",
    "15d4b9783977a6bf39f
  ",
    "4161710da9b030e9ed3
  ",
    "2f4352e36da85a9e4de
  ",
    "6ac059906743d02e377
  ",
    "358fd32e138a0052a13
  ",
    "624683afdf32fd28d46
  "
  ]
23:48:09   generate 1
23:48:09   [
    "57b88e3612491e3d5be
  "
  ]
```

Bitcoin - Incoming transaction

Date: 1/27/17 23:48
Amount: +12.49000000 BTC
Type: Mined
Address: mmY8o3Zi7pFUQyx49bepJSz5WGYgbMqYQe
Date: 1/27/17 23:48
Amount: +0.20990280 BTC
Type: Received with
Address: mwJhAMN4BVPXjQ17nZGSYDtA6WzRybbF8h

bitcoin : bitcoin-qt
sidechain : bitcoin-qt
Bitcoin Core - Wallet [regte
Bitcoin Core - Wallet [regte
Debug window
Details for d930f51822914
sidechain : bitcoin-qt — Kon
11:48 PM

Potential Sidechains

1. Hivemind – P2P Oracle System and Prediction-Asset Marketplace. Helps create and broadcast complex information, creates capital market efficiency, destroys scams and Ponzi schemes, and allows for certain kinds of insurance markets.
2. MimbleWimble – Hyper-specialized version of Bitcoin, less programmability, but features a 'magically' shrinking blockchain.
3. Rootstock – Reimplementation of Ethereum led by Bitcoin veteran and world-class security researcher SDL. Less self-deception, less dream-selling, less obfuscation, more "actual work" and "professional ethics".
4. Elements Project – Blockstream's laboratory for extremely technical and ambitious ideas.
5. SiaCoin – a P2P version of DropBox or Carbonite. Matches unused hard drive space to user who want backups.
6. Codex – Reimplementation of Namecoin. Potential to greatly improve internet safety, privacy, and reliability.

Potential Sidechains (cont.)

7. Monero – Greater transaction privacy, chain-wide.
8. Zcash – Privacy so extreme, no one really understands what's going on in here.
9. BitMessage – P2P messaging system emphasizing privacy. With 'hashcash' style fees, we might solve the spam problem and break Google's control over our digital lives.
10. Counterparty – Digital asset market, with P2P trades. These assets *may* be backed by TTPs to enable 'stocks on the blockchain' etc.
11. DropZone – Physical contraband market. Currently the production version plans to use Bitcoin Testnet for a variety of reasons.

Scaling Sidechain

- Presented about this in Milan – look it up!
- What is the Scaling Problem really about?
    - If x = resources required to run network (ie cost of full node, ie “block size”)
    - If y = network throughput (ie, “transactions per second”)
    - Then ratio r = y/x is the network’s scalability, which is affected by tech:
        - Lightning Network, Near Blocks / IBLTs, Pruning, Schnorr Signature Aggregation
- Scaling Debate is not about maximizing r, it is about “choosing the right x”!
- People disagree about x. With “wise contracts” and “blind merged mining” (see blog), sidechains can choose whatever x they like, without negatively impacting other chains at all.
- Sidechains…they solve everything!!

Thank You

paul.sztorc@bloq.com

drivechain.info