drivechains

sponsored by bloqLabs

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: monetary 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, because 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

KNOWING YOU'RE UNDER ATTACK

Learning that the Miner has Submitted Wrongly

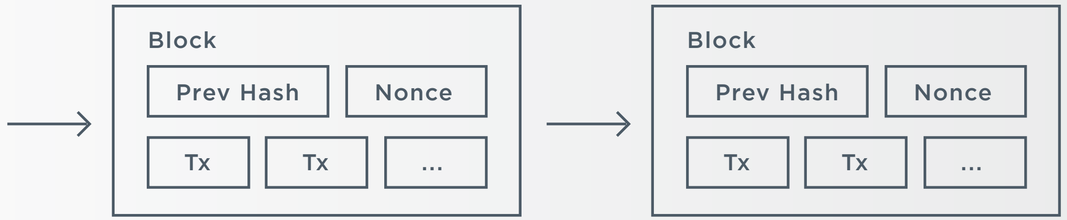
- We can only know by checking everything for ourselves (Positive Proof).
- But that isn't interesting! (No efficiency gain - effective hard fork).
- Alternatively, we can get very strong evidence against 'wrongness' if:
    - It is easy to sound the alarm on 'wrongness', easy to check the alarm...
    - ... 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 up the block 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

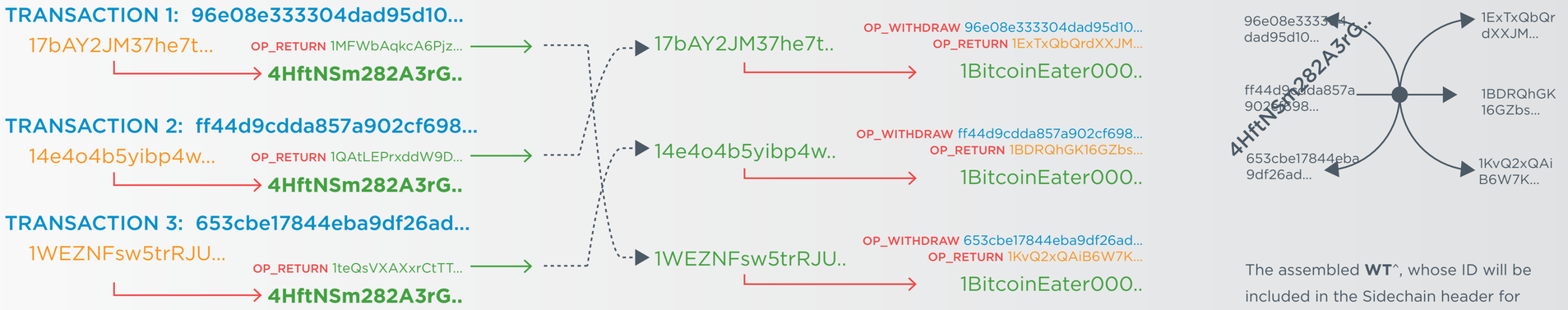
- **Now every attack will be:**
    1. Obvious to everyone (easy to observe that attack is happening).
    2. Deliberate (ie, inexcusable).
    3. “Unquenchable” (miner is not demanding something reasonable - instead asking for the ability to rob ***everyone***).
- **How might users react to such an 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)

SIDECHAIN
(VERY RECENT PAST)

SIDE-TO-MAIN
(AT PRESENT)

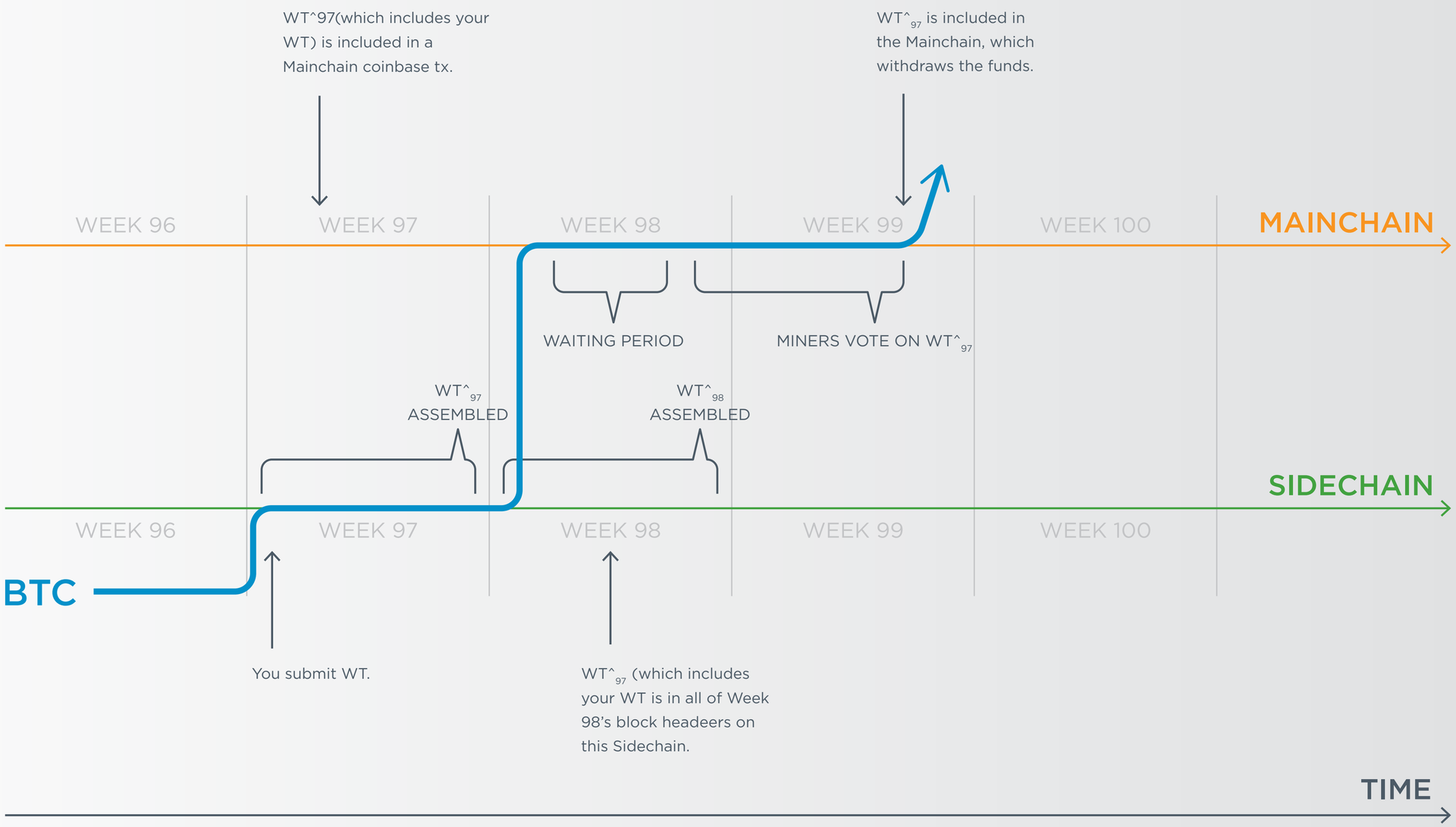


Three deposits, from Bitcoin **orange** to an address **green** on a Bitcoin sidechain **bold green**. The Mainchain BTC are trapped “in **4HftNSm282A3rG..**”.

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

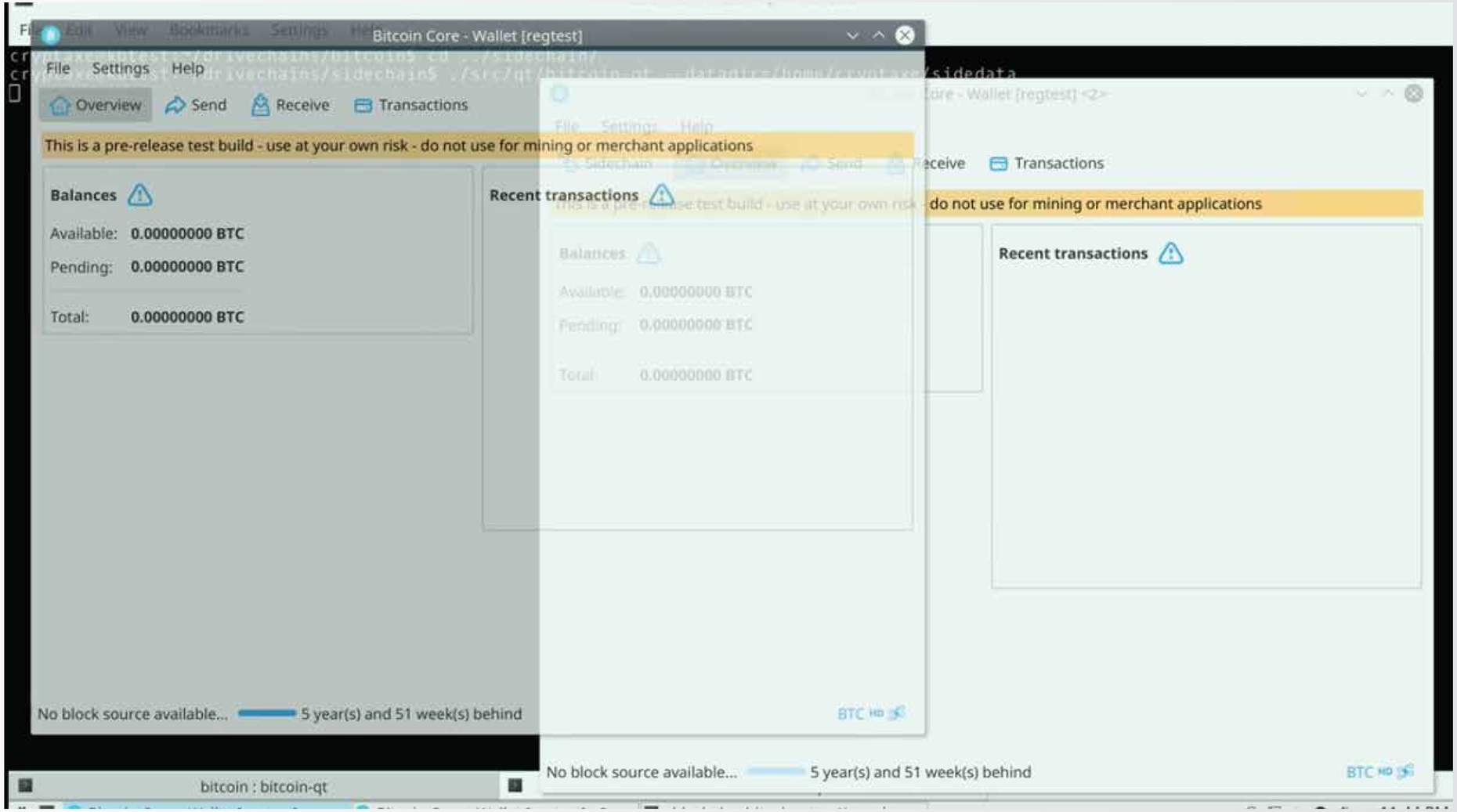
The assembled **WT**^, whose ID will be included in the Sidechain header for a while. On the Bitcoin Mainchain, it eventually moves BTC “from **4HftNSm282A3rG..**” to their new owners.

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


WT^97(which includes your WT) is included in a Mainchain coinbase tx.
WT^97 is included in the Mainchain, which withdraws the funds.
WEEK 96
WEEK 97
WEEK 98
WEEK 99
WEEK 100
MAINCHAIN
WAITING PERIOD
MINERS VOTE ON WT^97
WT^97 ASSEMBLED
WT^98 ASSEMBLED
SIDECHAIN
WEEK 96
WEEK 97
WEEK 98
WEEK 99
WEEK 100
BTC
You submit WT.
WT^97 (which includes your WT is in all of Week 98's block headeers on this Sidechain.
TIME

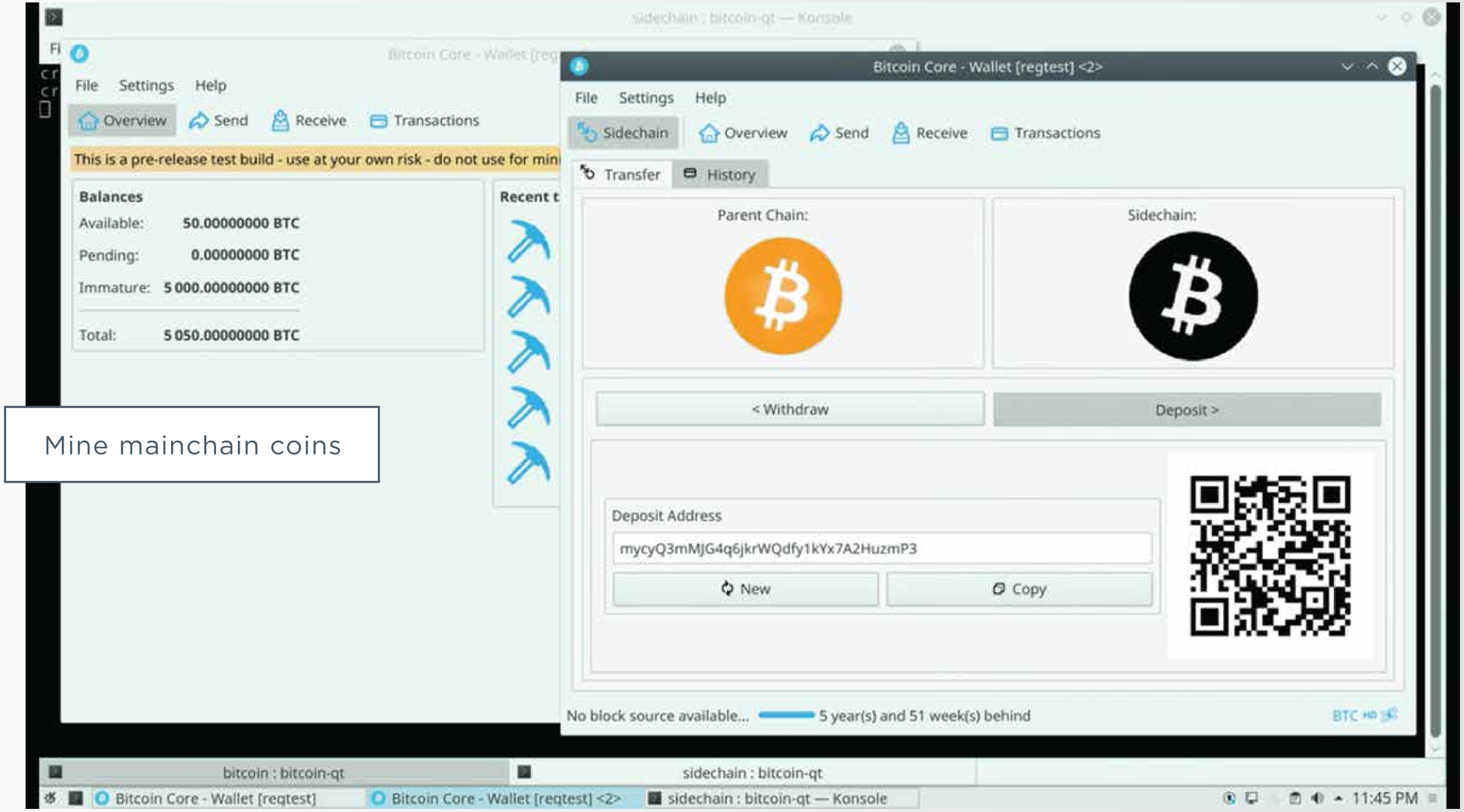
Two Bitcoin Windows

Full video at drivechain.info



Sidechain GUI

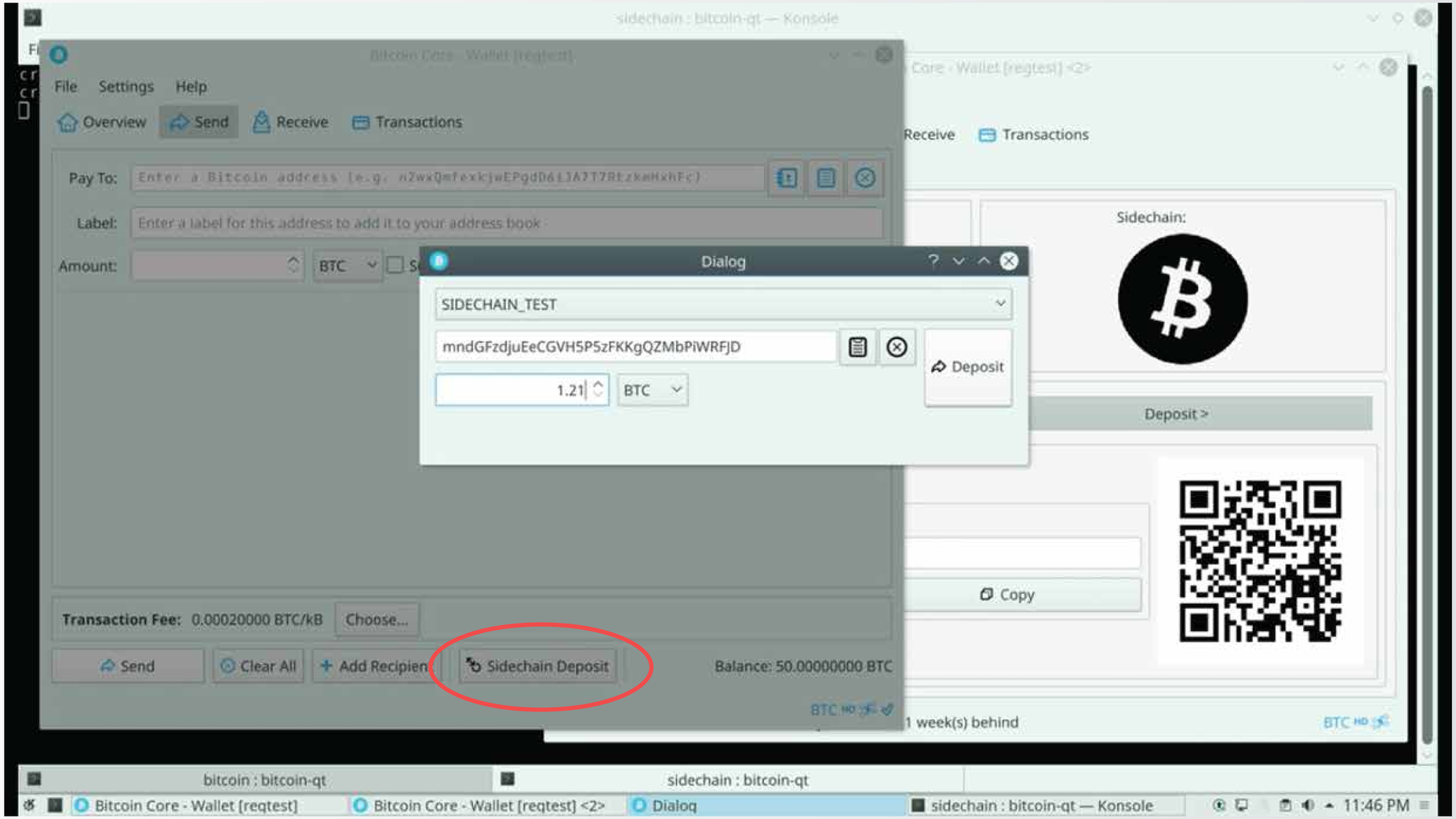
Full video at drivechain.info



Mine mainchain coins

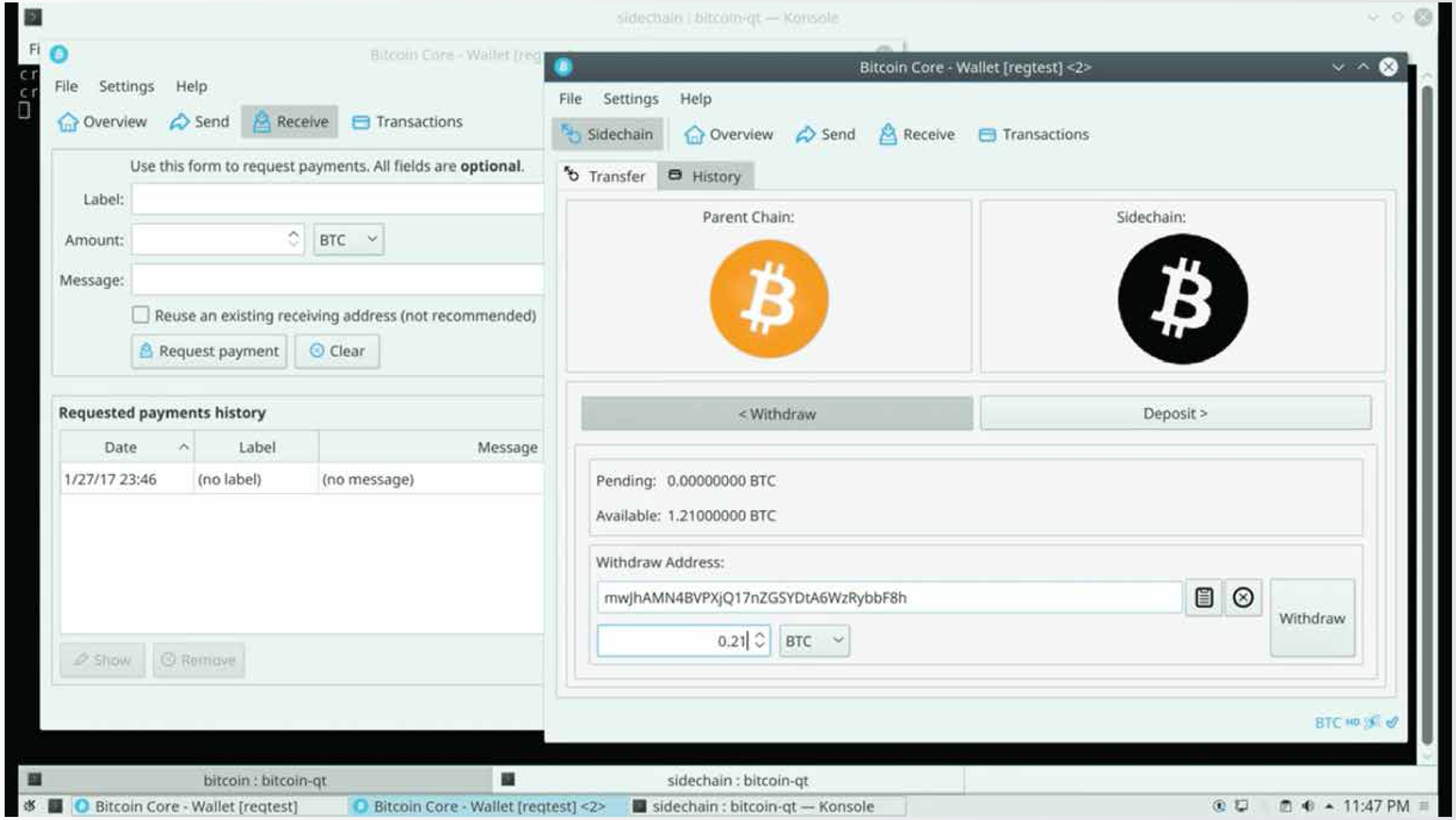
Deposit Coins to Sidechain

Full video at drivechain.info

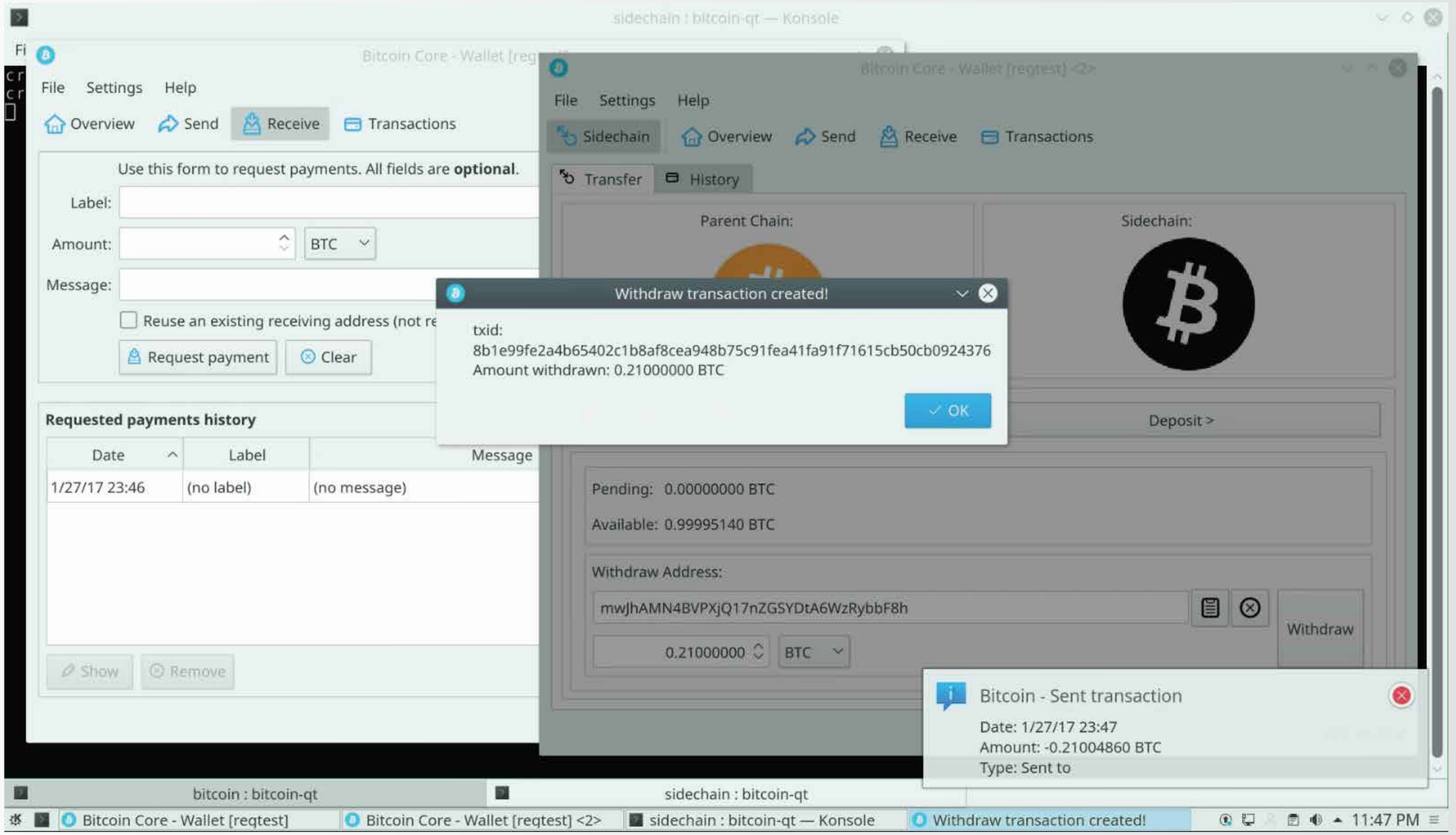


Take the Deposit & Withdraw It Back to Mainchain

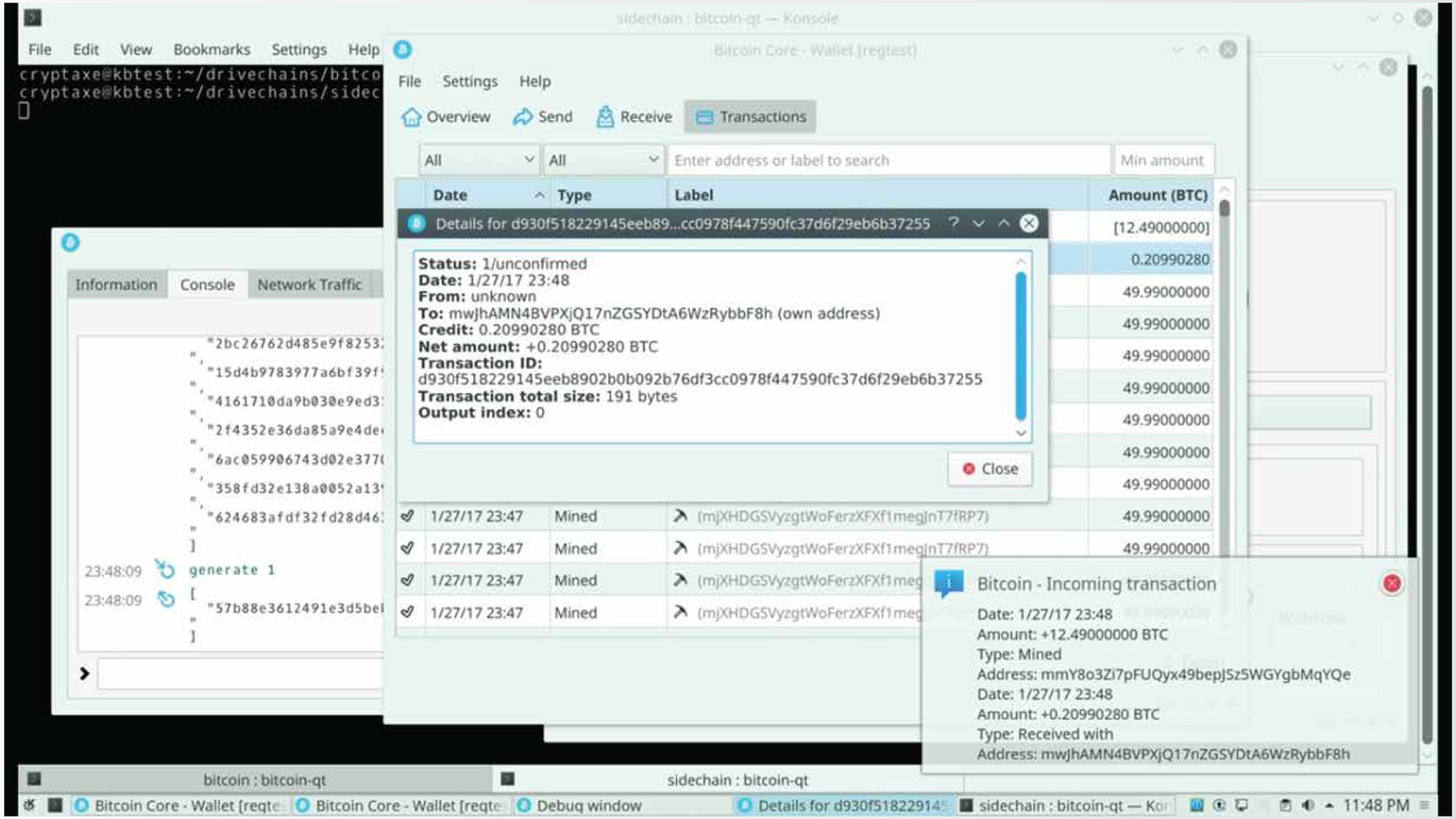
Full video at drivechain.info



Full video at drivechain.info



Full video at drivechain.info



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”.

POTENTIAL SIDECHAINS (continued)

4. **Elements Project –** Blockstream'slaboratory for extremely technical and ambitious ideas.

5. **SiaCoin –** a P2P version of DropBoxor 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.

7. **Monero –** Greater transaction privacy, chain-wide.

POTENTIAL SIDECHAINS (continued)

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 Testnetfor 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