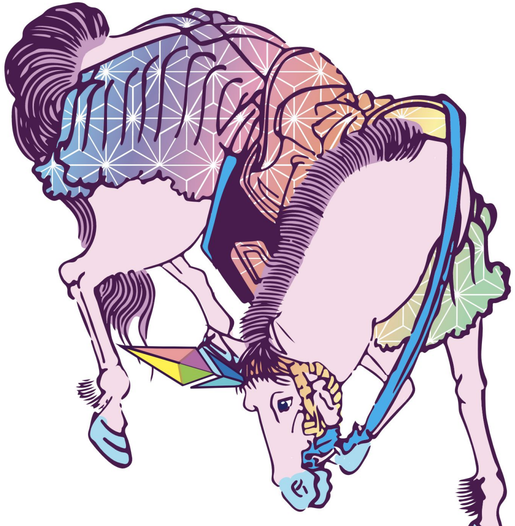
SIDECHAINS ARE NOT LAYER 2



Georgios Konstantopoulos
Independent Consultant & Researcher
Twitter: @gakonst / me@gakonst.com

Slides available: gakonst.com/sidechains2019.pdf

Where it all started.

Enabling Blockchain Innovations with Pegged Sidechains

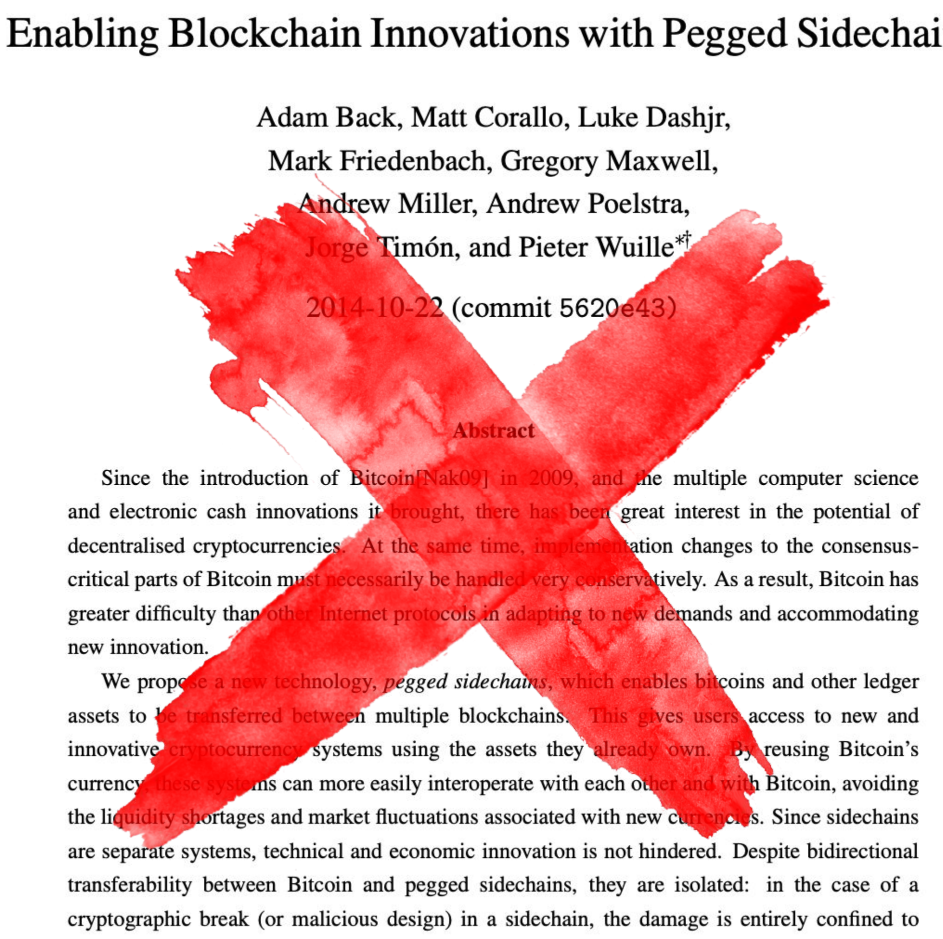
Adam Back, Matt Corallo, Luke Dashjr,
Mark Friedenbach, Gregory Maxwell,
Andrew Miller, Andrew Poelstra,
Jorge Timón, and Pieter Wuille[*†]

2014-10-22 (commit 5620e43)

Abstract

Since the introduction of Bitcoin[Nak09] in 2009, and the multiple computer science and electronic cash innovations it brought, there has been great interest in the potential of decentralised cryptocurrencies. At the same time, implementation changes to the consensus-critical parts of Bitcoin must necessarily be handled very conservatively. As a result, Bitcoin has greater difficulty than other Internet protocols in adapting to new demands and accommodating new innovation.

We propose a new technology, *pegged sidechains*, which enables bitcoins and other ledger assets to be transferred between multiple blockchains. This gives users access to new and innovative cryptocurrency systems using the assets they already own. By reusing Bitcoin's currency, these systems can more easily interoperate with each other and with Bitcoin, avoiding the liquidity shortages and market fluctuations associated with new currencies. Since sidechains are separate systems, technical and economic innovation is not hindered. Despite bidirectional transferability between Bitcoin and pegged sidechains, they are isolated: in the case of a cryptographic break (or malicious design) in a sidechain, the damage is entirely confined to



Enabling Blockchain Innovations with Pegged Sidechains

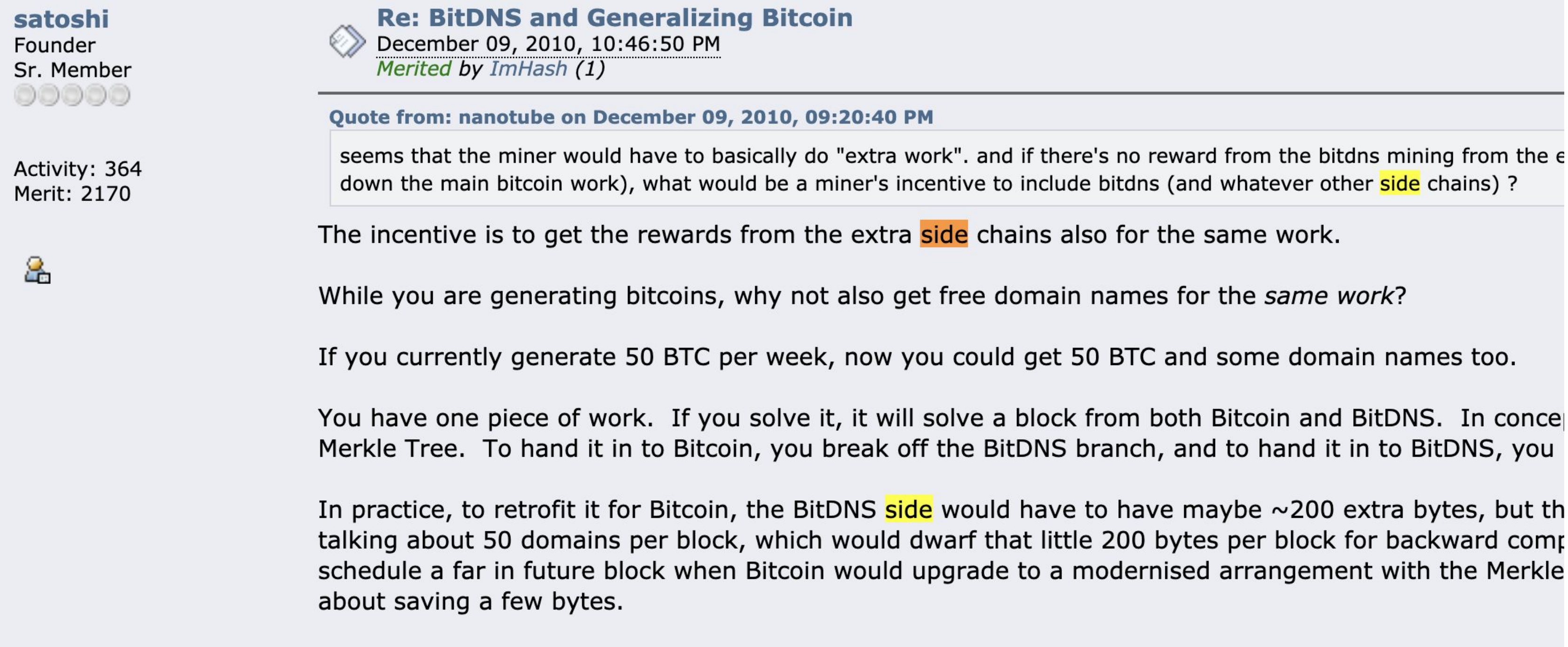
Adam Back, Matt Corallo, Luke Dashjr,
Mark Friedenbach, Gregory Maxwell,
Andrew Miller, Andrew Poelstra,
Jorge Timón, and Pieter Wuille*†

2014-10-22 (commit 5620e43)

Abstract

Since the introduction of Bitcoin[Nak09] in 2009, and the multiple computer science and electronic cash innovations it brought, there has been great interest in the potential of decentralised cryptocurrencies. At the same time, implementation changes to the consensus-critical parts of Bitcoin must necessarily be handled very conservatively. As a result, Bitcoin has greater difficulty than other Internet protocols in adapting to new demands and accommodating new innovation.

We propose a new technology, *pegged sidechains*, which enables bitcoins and other ledger assets to be transferred between multiple blockchains. This gives users access to new and innovative cryptocurrency systems using the assets they already own. By reusing Bitcoin's currency, these systems can more easily interoperate with each other and with Bitcoin, avoiding the liquidity shortages and market fluctuations associated with new currencies. Since sidechains are separate systems, technical and economic innovation is not hindered. Despite bidirectional transferability between Bitcoin and pegged sidechains, they are isolated: in the case of a cryptographic break (or malicious design) in a sidechain, the damage is entirely confined to



satoshi
Founder
Sr. Member

Activity: 364
Merit: 2170

Re: BitDNS and Generalizing Bitcoin
December 09, 2010, 10:46:50 PM
Merited by ImHash (1)

Quote from: nanotube on December 09, 2010, 09:20:40 PM

> seems that the miner would have to basically do "extra work". and if there's no reward from the bitdns mining from the e
> down the main bitcoin work), what would be a miner's incentive to include bitdns (and whatever other side chains) ?

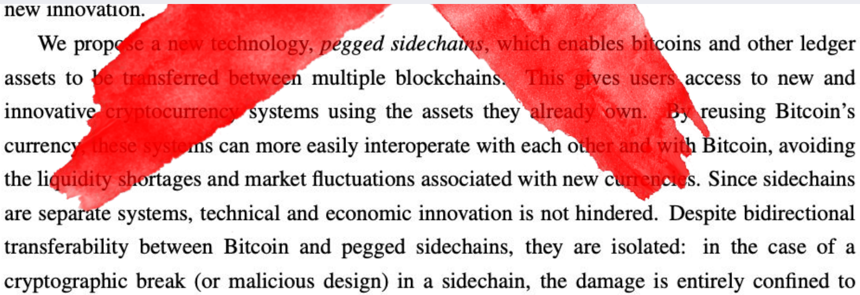
The incentive is to get the rewards from the extra side chains also for the same work.

While you are generating bitcoins, why not also get free domain names for the *same work*?

If you currently generate 50 BTC per week, now you could get 50 BTC and some domain names too.

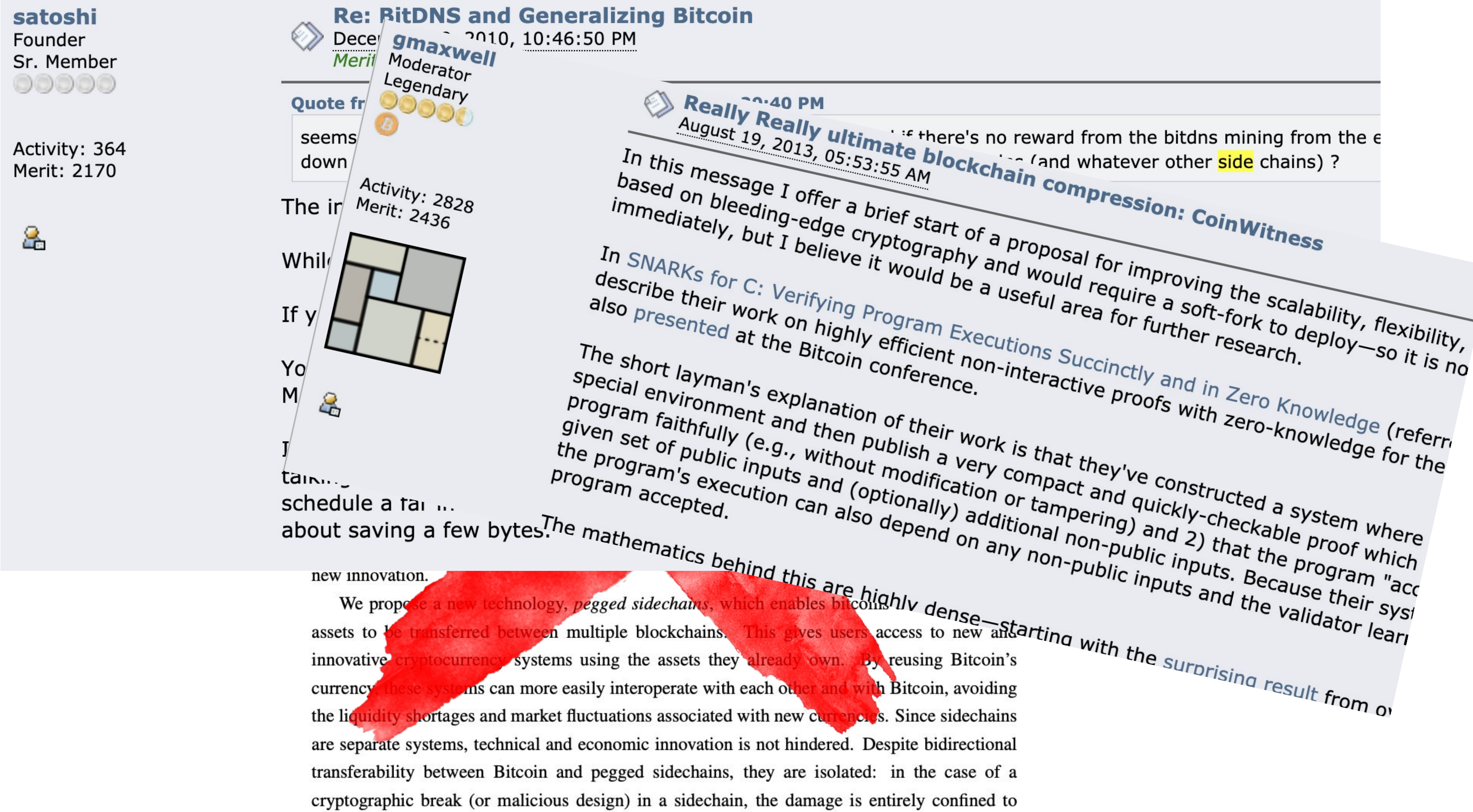
You have one piece of work. If you solve it, it will solve a block from both Bitcoin and BitDNS. In conce
Merkle Tree. To hand it in to Bitcoin, you break off the BitDNS branch, and to hand it in to BitDNS, you

In practice, to retrofit it for Bitcoin, the BitDNS side would have to have maybe ~200 extra bytes, but th
talking about 50 domains per block, which would dwarf that little 200 bytes per block for backward comp
schedule a far in future block when Bitcoin would upgrade to a modernised arrangement with the Merkle
about saving a few bytes.



new innovation.

We propose a new technology, *pegged sidechains*, which enables bitcoins and other ledger assets to be transferred between multiple blockchains. This gives users access to new and innovative cryptocurrency systems using the assets they already own. By reusing Bitcoin's currency, these systems can more easily interoperate with each other and with Bitcoin, avoiding the liquidity shortages and market fluctuations associated with new currencies. Since sidechains are separate systems, technical and economic innovation is not hindered. Despite bidirectional transferability between Bitcoin and pegged sidechains, they are isolated: in the case of a cryptographic break (or malicious design) in a sidechain, the damage is entirely confined to



satoshi
Founder
Sr. Member

Activity: 364
Merit: 2170

Re: BitDNS and Generalizing Bitcoin
Dece 2010, 10:46:50 PM
Merit

Quote fr 0:40 PM
seems if there's no reward from the bitdns mining from the e
down (and whatever other side chains) ?

The ir

Whil

If y

Yo
M

I
talki
schedule a fai
about saving a few bytes.

gmaxwell
Moderator
Legendary

Activity: 2828
Merit: 2436

Really Really ultimate blockchain compression: CoinWitness
August 19, 2013, 05:53:55 AM

In this message I offer a brief start of a proposal for improving the scalability, flexibility, based on bleeding-edge cryptography and would require a soft-fork to deploy—so it is no immediately, but I believe it would be a useful area for further research.

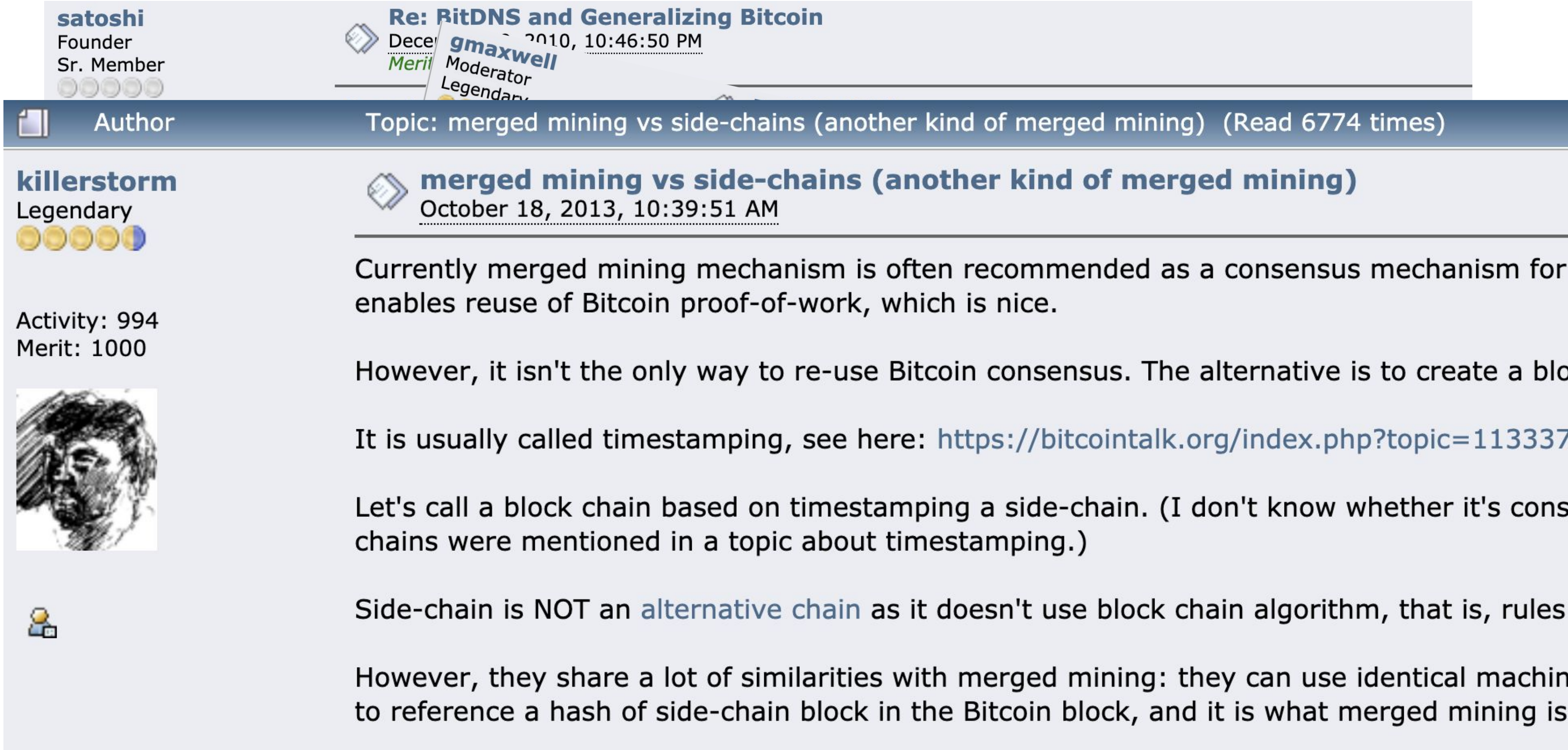
In SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge (referr describe their work on highly efficient non-interactive proofs with zero-knowledge for the also presented at the Bitcoin conference.

The short layman's explanation of their work is that they've constructed a system where special environment and then publish a very compact and quickly-checkable proof which program faithfully (e.g., without modification or tampering) and 2) that the program "acc given set of public inputs and (optionally) additional non-public inputs. Because their syst the program's execution can also depend on any non-public inputs and the validator lear program accepted.

The mathematics behind this are highly dense—starting with the surprising result from o

new innovation.

We propose a new technology, *pegged sidechains*, which enables bitcoins assets to be transferred between multiple blockchains. This gives users access to new and innovative cryptocurrency systems using the assets they already own. By reusing Bitcoin's currency, these systems can more easily interoperate with each other and with Bitcoin, avoiding the liquidity shortages and market fluctuations associated with new currencies. Since sidechains are separate systems, technical and economic innovation is not hindered. Despite bidirectional transferability between Bitcoin and pegged sidechains, they are isolated: in the case of a cryptographic break (or malicious design) in a sidechain, the damage is entirely confined to



satoshi
Founder
Sr. Member

Re: BitDNS and Generalizing Bitcoin
Dece 2010, 10:46:50 PM
Merit

gmaxwell
Moderator
Legendar

Author | Topic: merged mining vs side-chains (another kind of merged mining) (Read 6774 times)

killerstorm
Legendary

Activity: 994
Merit: 1000

merged mining vs side-chains (another kind of merged mining)
October 18, 2013, 10:39:51 AM

Currently merged mining mechanism is often recommended as a consensus mechanism for
enables reuse of Bitcoin proof-of-work, which is nice.

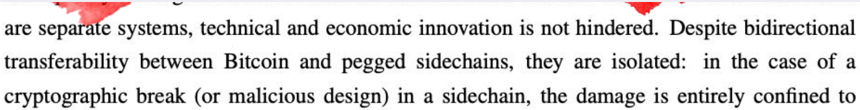
However, it isn't the only way to re-use Bitcoin consensus. The alternative is to create a blo

It is usually called timestamping, see here: https://bitcointalk.org/index.php?topic=11333

Let's call a block chain based on timestamping a side-chain. (I don't know whether it's cons
chains were mentioned in a topic about timestamping.)

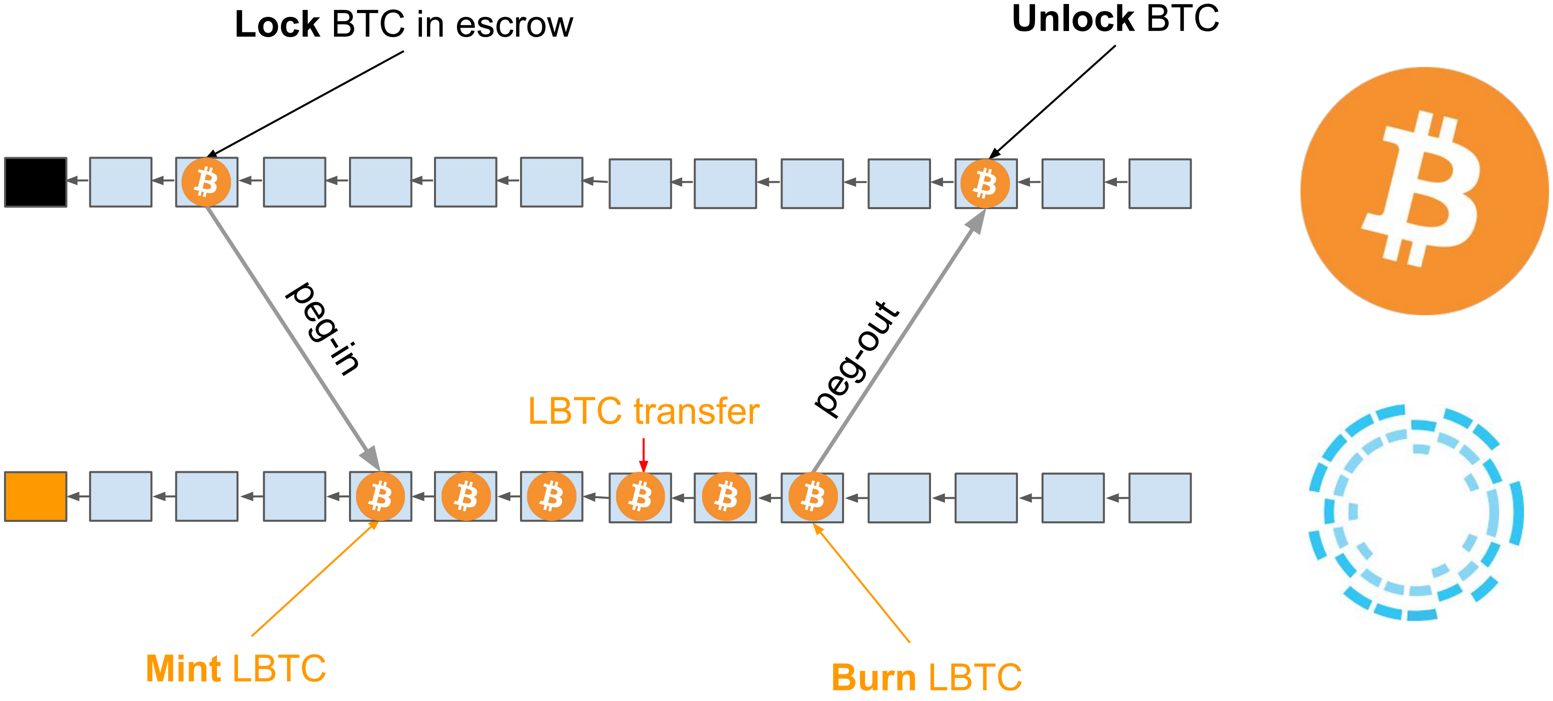
Side-chain is NOT an alternative chain as it doesn't use block chain algorithm, that is, rules

However, they share a lot of similarities with merged mining: they can use identical machin
to reference a hash of side-chain block in the Bitcoin block, and it is what merged mining is



are separate systems, technical and economic innovation is not hindered. Despite bidirectional transferability between Bitcoin and pegged sidechains, they are isolated: in the case of a cryptographic break (or malicious design) in a sidechain, the damage is entirely confined to

The 2-way peg

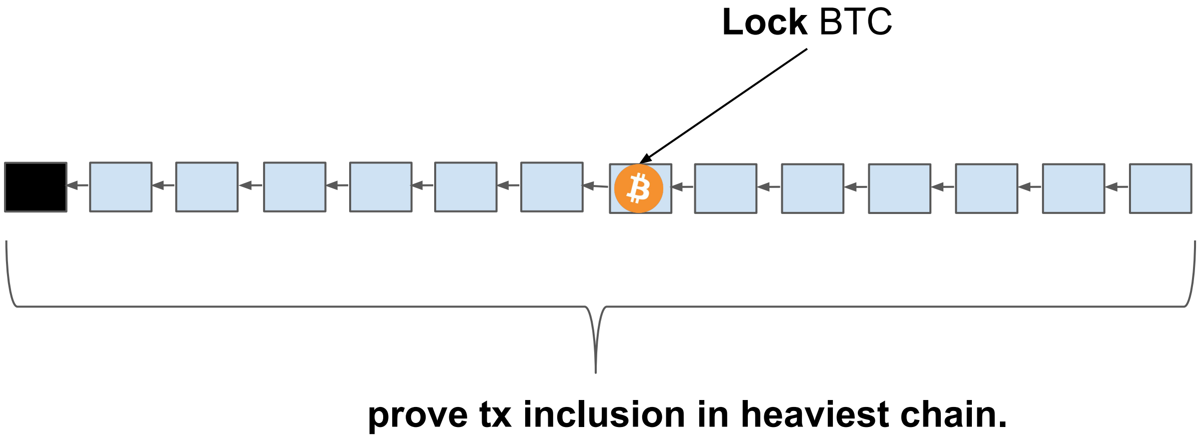

Lock BTC in escrow
Unlock BTC
peg-in
peg-out
LBTC transfer
Mint LBTC
Burn LBTC

How can a chain objectively observe another chain’s state?

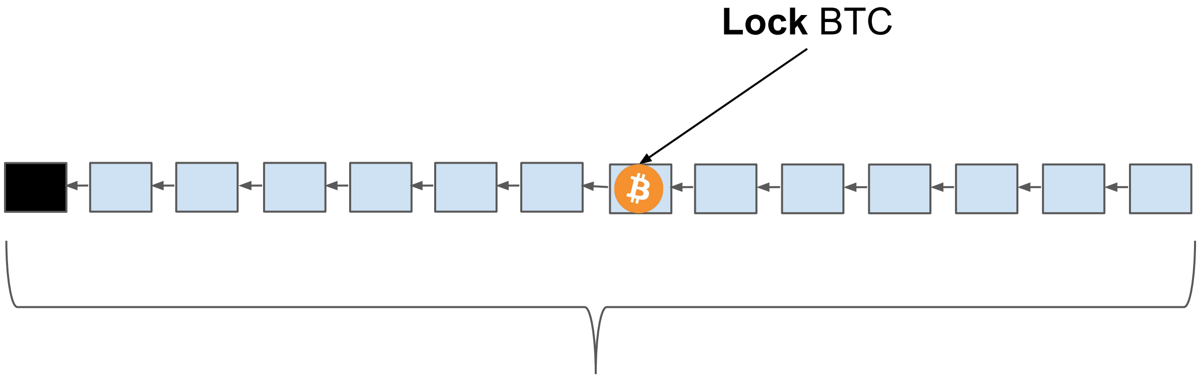
Work*!

*as long as we can verify the other chain's PoW algorithm.
Litecoin's scrypt → 20m gas on EVM 🤔

Simple Payment Verification - like a light client!



Simple Payment Verification - like a light client!



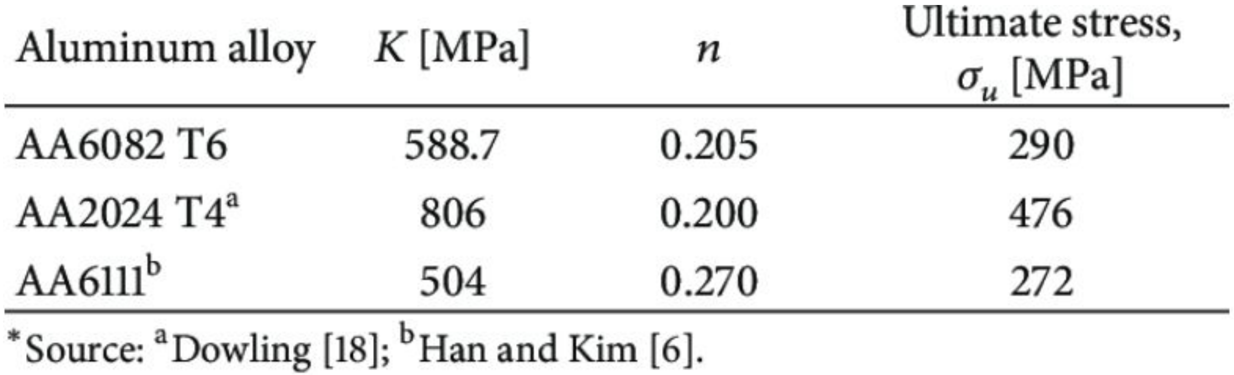
prove tx inclusion in heaviest chain

O(n), too expensive.
→ NiPoPoWs / SNARKs / Stateless SPV

all work is not equal:

2-way pegs without a reliable peg-out mechanism are not useful.

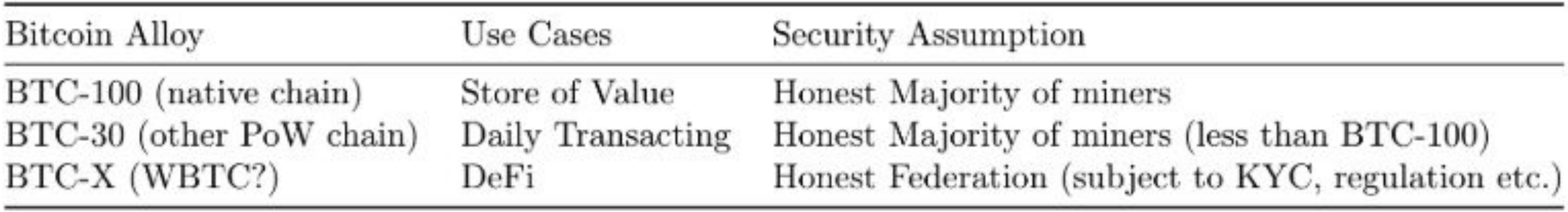
cross-chain assets = alloys.



Aluminum alloy	K [MPa]	n	Ultimate stress, σ_u [MPa]
AA6082 T6	588.7	0.205	290
AA2024 T4[a]	806	0.200	476
AA6111[b]	504	0.270	272

*Source: [a]Dowling [18]; [b]Han and Kim [6].

cross-chain assets = alloys.



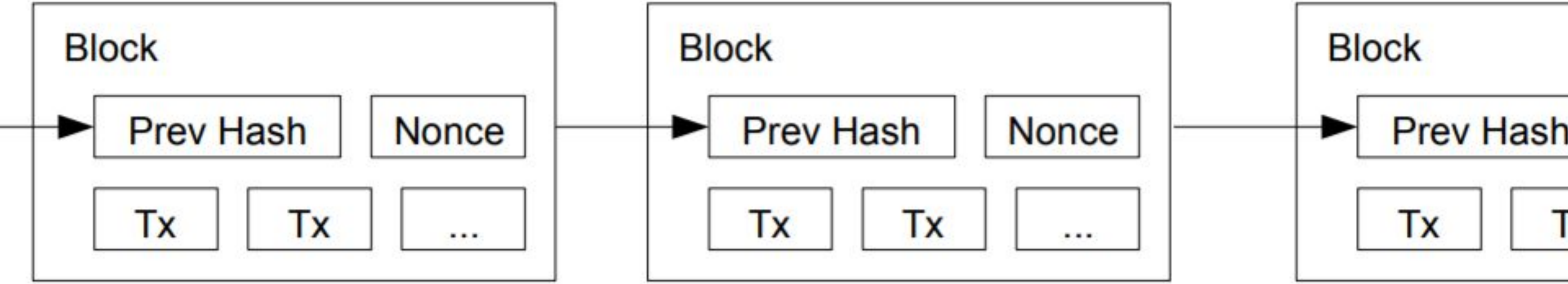
Bitcoin Alloy	Use Cases	Security Assumption
BTC-100 (native chain)	Store of Value	Honest Majority of miners
BTC-30 (other PoW chain)	Daily Transacting	Honest Majority of miners (less than BTC-100)
BTC-X (WBTC?)	DeFi	Honest Federation (subject to KYC, regulation etc.)

Proof of Stake sidechains?

Proof of Stake sidechains?

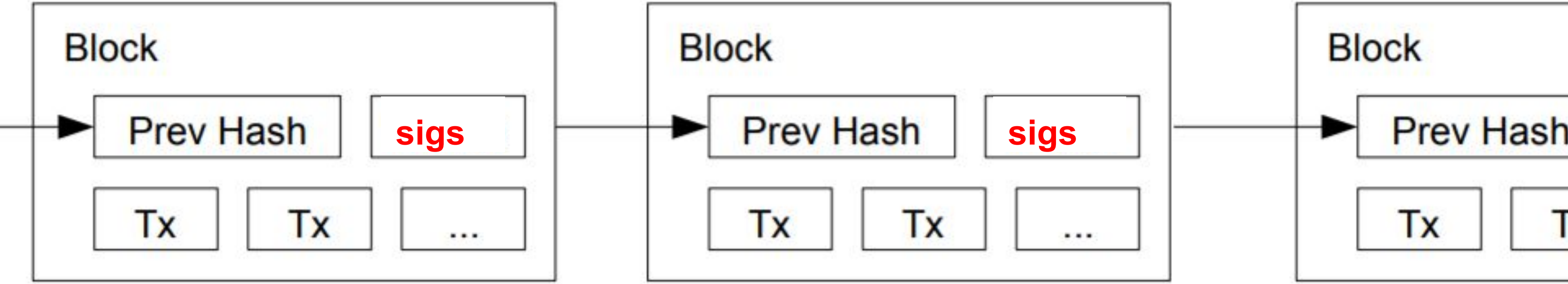
Proof of Stake light-clients?

Proof of Work block



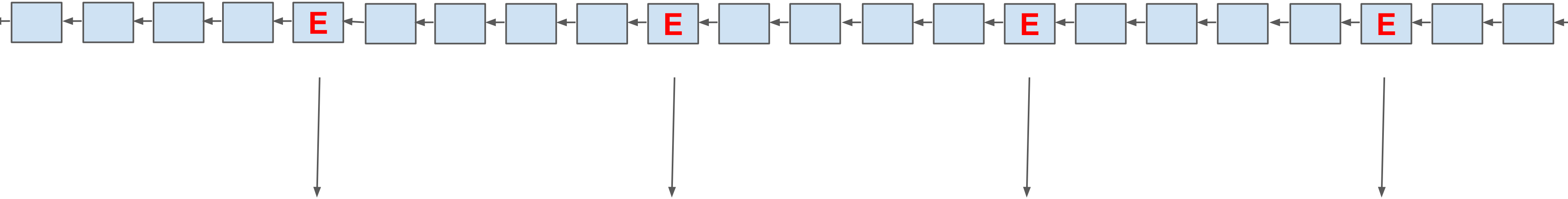
accept if h(block) < T

Proof of Stake block



accept if stake(sigs) > ⅔ total stake

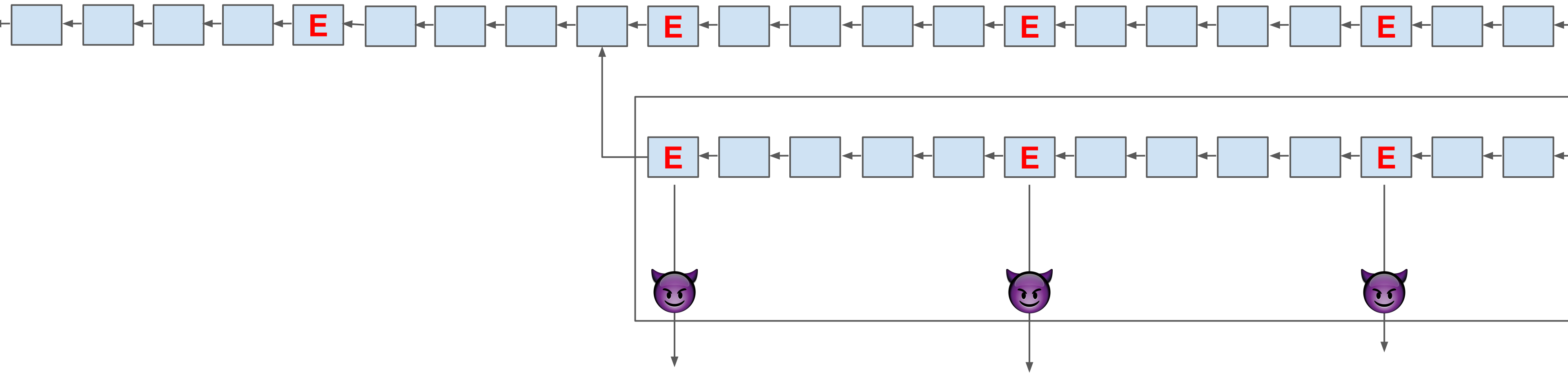
Proof of Proof of Stake: Verify aggregate signature each time the validator set changes



O(n) for “linear” light clients
+ sidechain smart contract must have
latest stake distribution

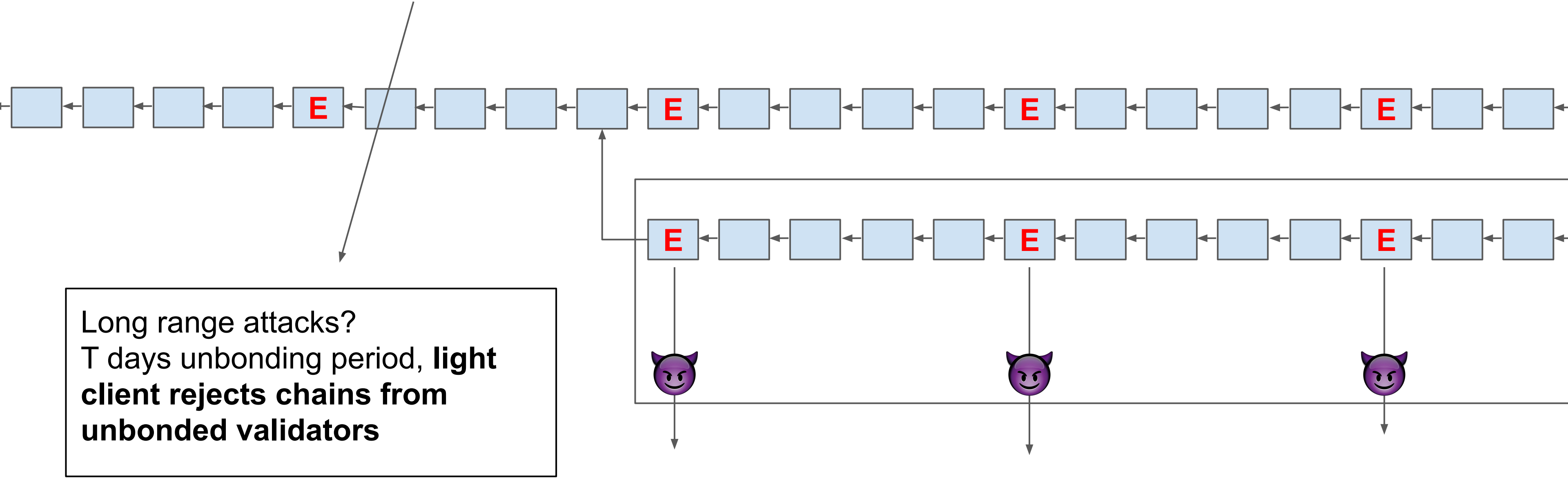
“Cross-chain nothing-at-stake attack”

1. Feed light client with bad fork
2. Light client broadcasts fake-chain to 1 honest validator & slashes equivocators



“Cross-chain nothing-at-stake attack”

1. **Feed** light client with bad fork
2. Light client broadcasts fake-chain to 1 honest validator & **slashes equivocators**

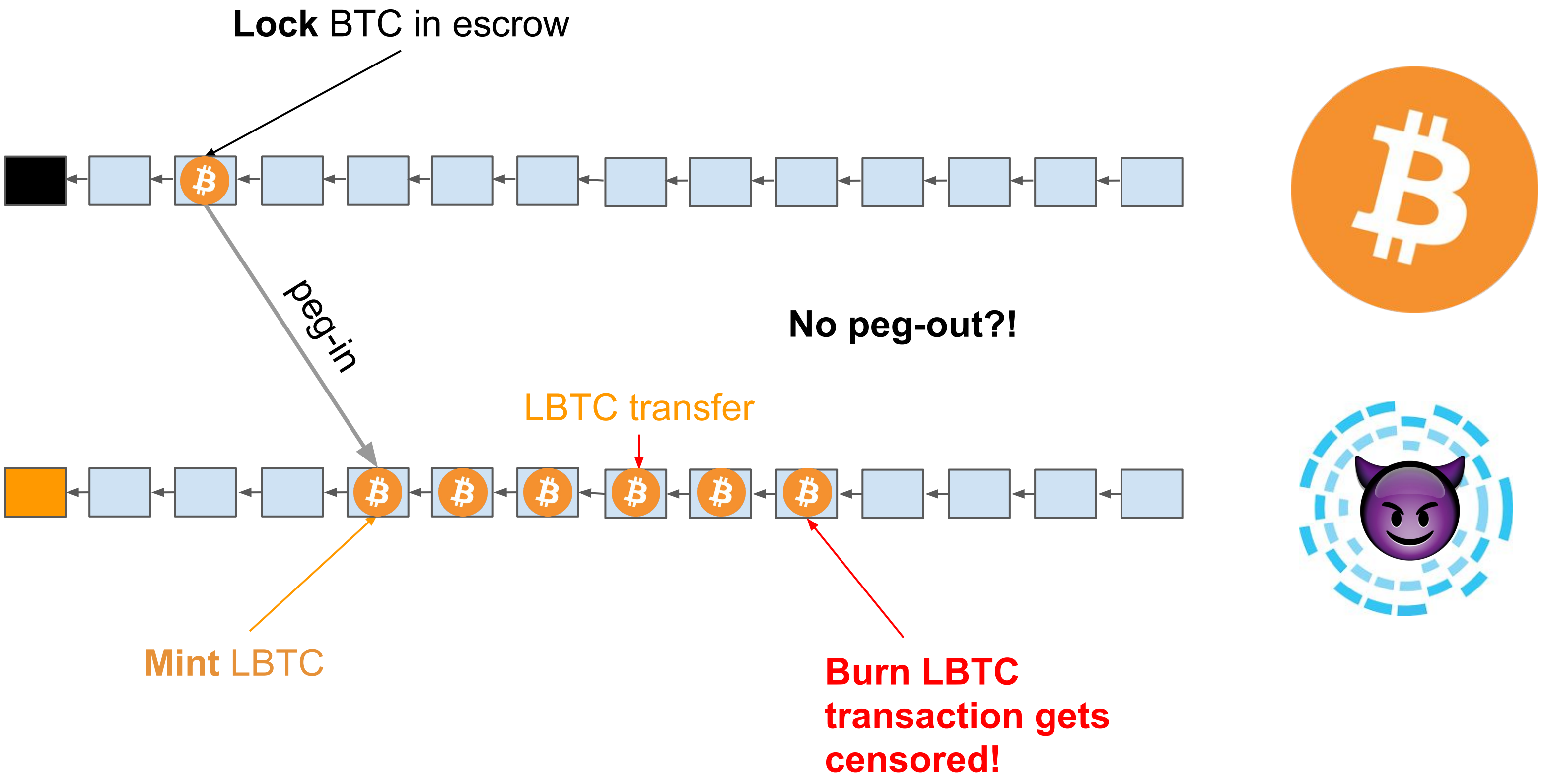


Long range attacks?
T days unbonding period, **light client rejects chains from unbonded validators**

everything so far
assumes that both chains are secure.

secure == expensive
expensive != scalable

Sidechains considered harmful



Lock BTC in escrow

peg-in

No peg-out?!

LBTC transfer

Mint LBTC

Burn LBTC transaction gets censored!

Peg-in / Peg-out taxonomy

	Peg-in / Peg-out
Federated	Multisig
PoW Sidechain	NiPoPoWs + reorg proofs
PoS Sidechain	Rotating multisig weighted by stake + equivocation slashing

Must trade security for scalability

SoK: Communication Across Distributed Ledgers
https://eprint.iacr.org/2019/1128.pdf

Sidechains:

- **interoperability** solution
- **NOT** a **scalability** solution
- **independent** security model
- consist of their own **L1 that talks with other L1s**

OK, how do we scale?

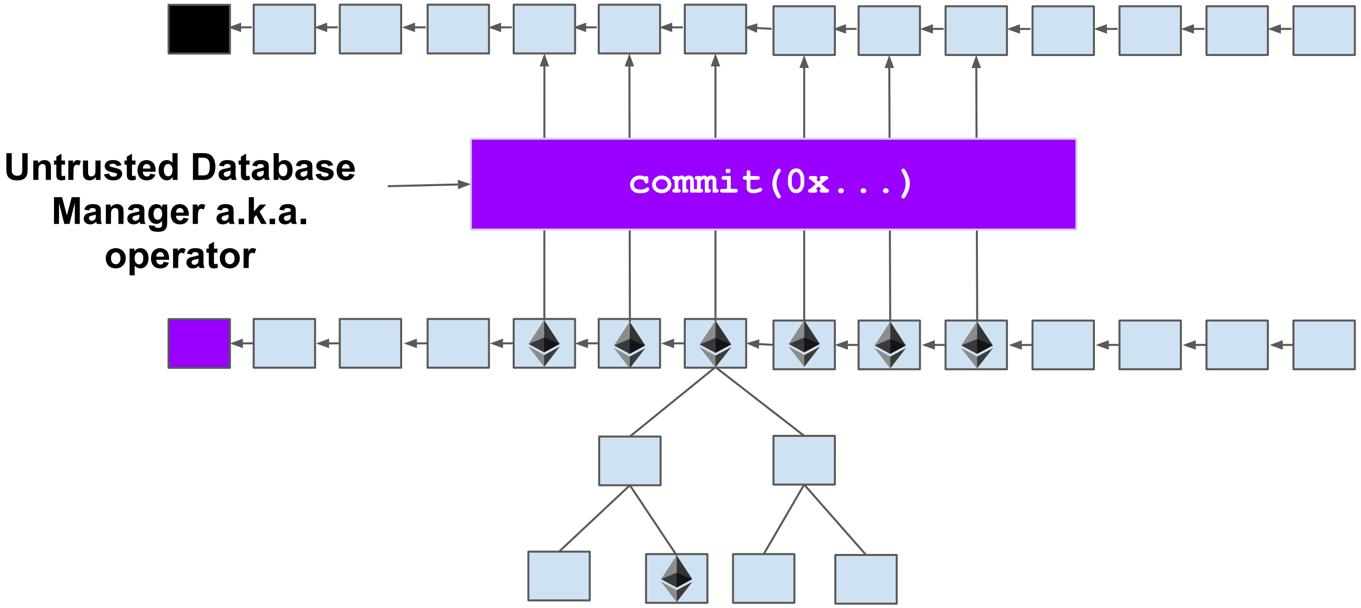
Layer 2! Off-chain!
On-chain minimalism!

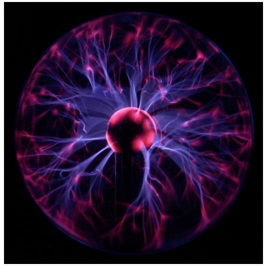
Making sense of Layer 2

1. State Channels
2. **Non-custodial sidechains / “commitchains”**

(great talk by Josh Stark at Devcon4)

Plasma - the first commitchain

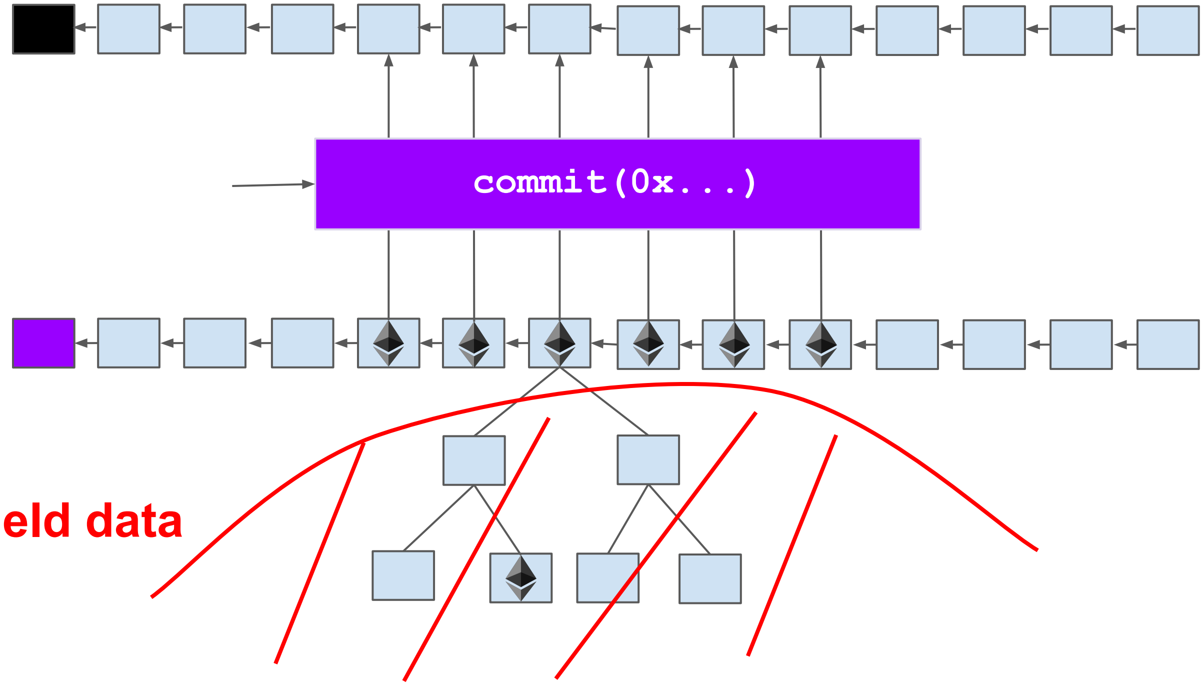




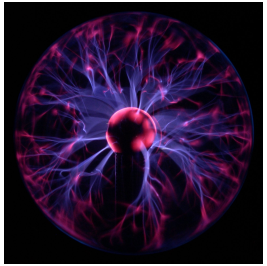
Commitchains inherit security from the L1

(under synchrony assumption for fraud proofs)

The problem with plasma



Withheld data



Plasma might’ve been a premature optimization.

Data unavailability is hard.

Off-chain computation

+ Off-chain data

+ Fraud Proofs

= Plasma

Off-chain computation

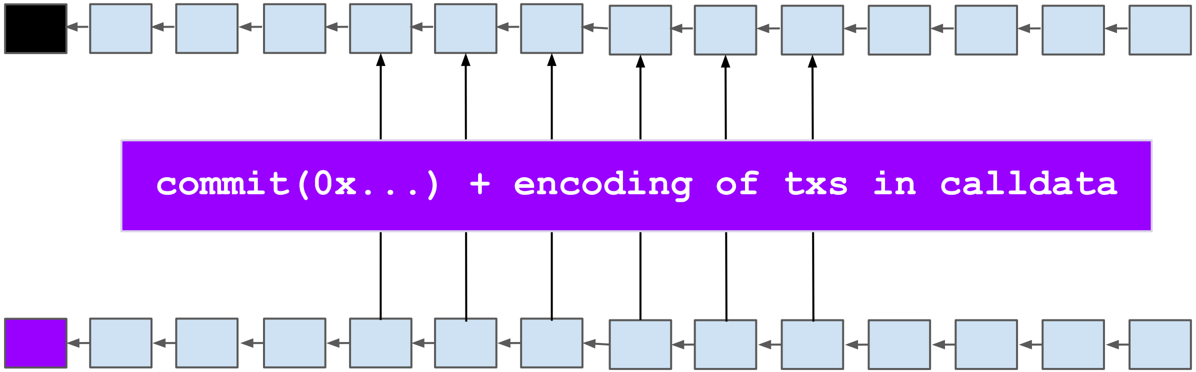
+ On-chain data

+ Fraud Proofs

= “Optimistic Rollup”

“Optimistic Rollup” - Put all the data on-chain

(aka Merged Consensus by Mikerah & John Adler)



Use the Layer 1 as a data availability and dispute layer. Do not perform any computations on the txs themselves.

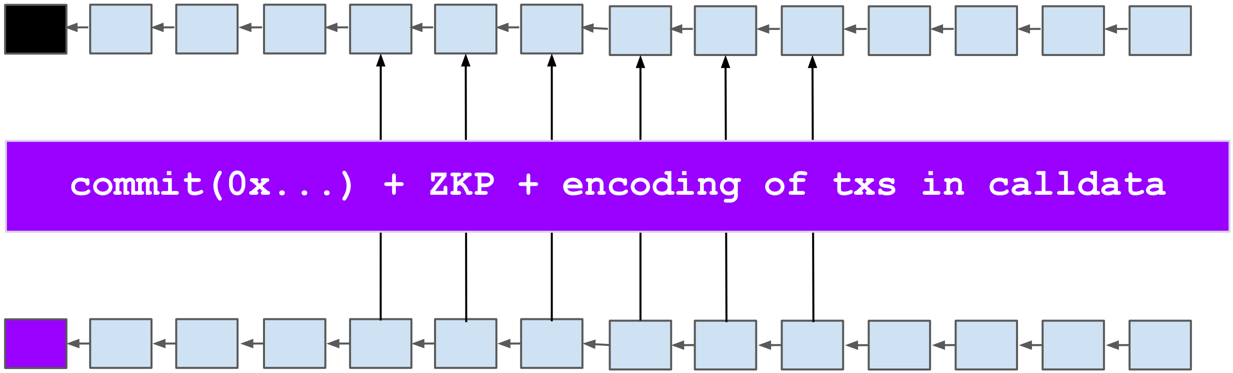
Off-chain computation

+ On-chain data

+ Validity Proofs

= "ZK Rollup"

“ZK Rollup”: ZKP + Put all the data on-chain



commit(0x...) + ZKP + encoding of txs in calldata

Fraud is prevented by the validity proof.

Validity Proof caveat: expensive, slow, maybe trusted setup

A note on on-chain data availability

1. “Solves” data availability problem → **#DeFi on L2?**
2. EIP2028 makes it cheaper!

Caveat:

1. Throughput capped at L1 capacity → O(1) improvement
2. “Parasitic”: Using a rollup means other apps are less usable
3. Whatever happened to on-chain minimalism?

https://vitalik.ca/general/2019/08/28/hybrid_layer_2.html

Takeaways & Commitchain Taxonomy

1. We know how to do PoW and PoS sidechains
2. Each sidechain **must** be individually secure
3. L2 **inherits** security from L1

	Checkpoint Integrity	**Withdrawal Integrity**	**Data Availability**	**Online Requirement?**	**Smart Contracts?**
Plasma	Detect & Exit	Fraud Proof	Wait for off-chain data	Yes	No?
Optimistic Rollup	Fraud proof	Fraud Proof	Post on-chain	Yes	Yes
ZK Rollup	ZKP	1 honest party (block producer)	Post on-chain	No	Yes

https://docs.google.com/presentation/d/1WnGzEf_tpIkzdRymgusEbyyoRmGbQmS5g9GsdIii0pU/

Sidechains are for interoperability

Layer 2 is for scalability

Sidechains

ARE NOT

Layer 2

Thank you for your attention

Q & A ?

@gakonst / me@gakonst.com

gakonst.com/scalingbitcoin2019.pdf

gakonst.com/plasmacash.pdf

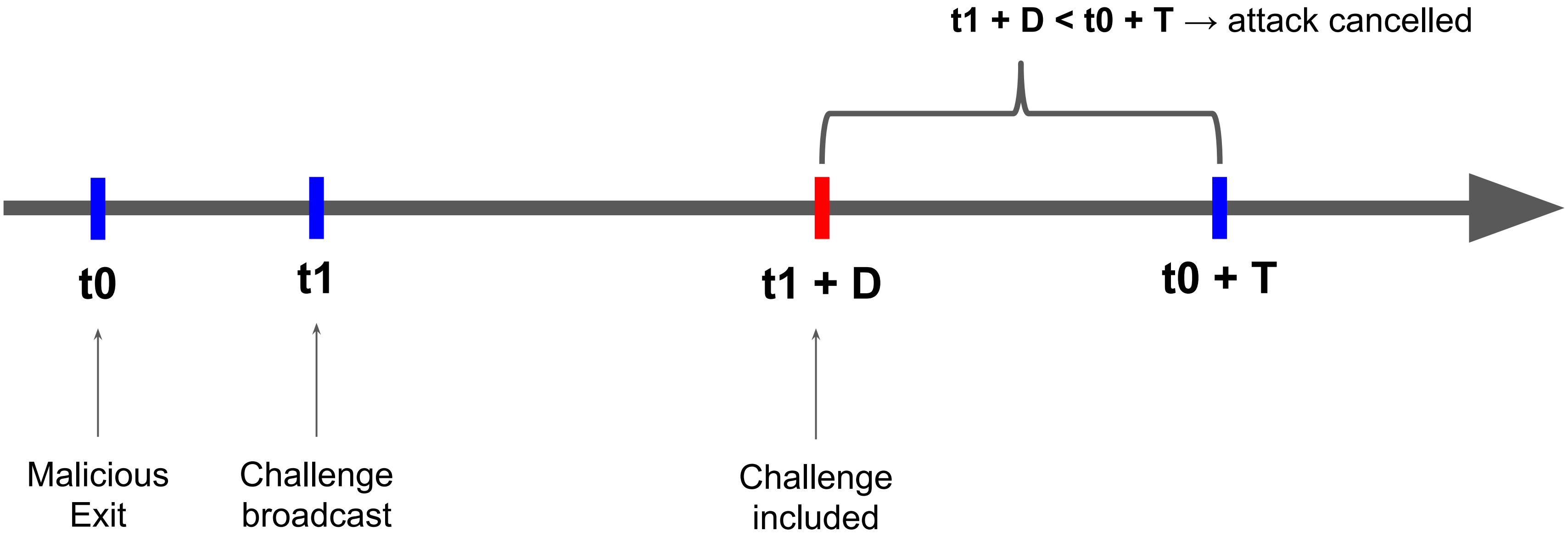
appendix

Security & Incentive Compatibility of Layer 2 games requirements*:

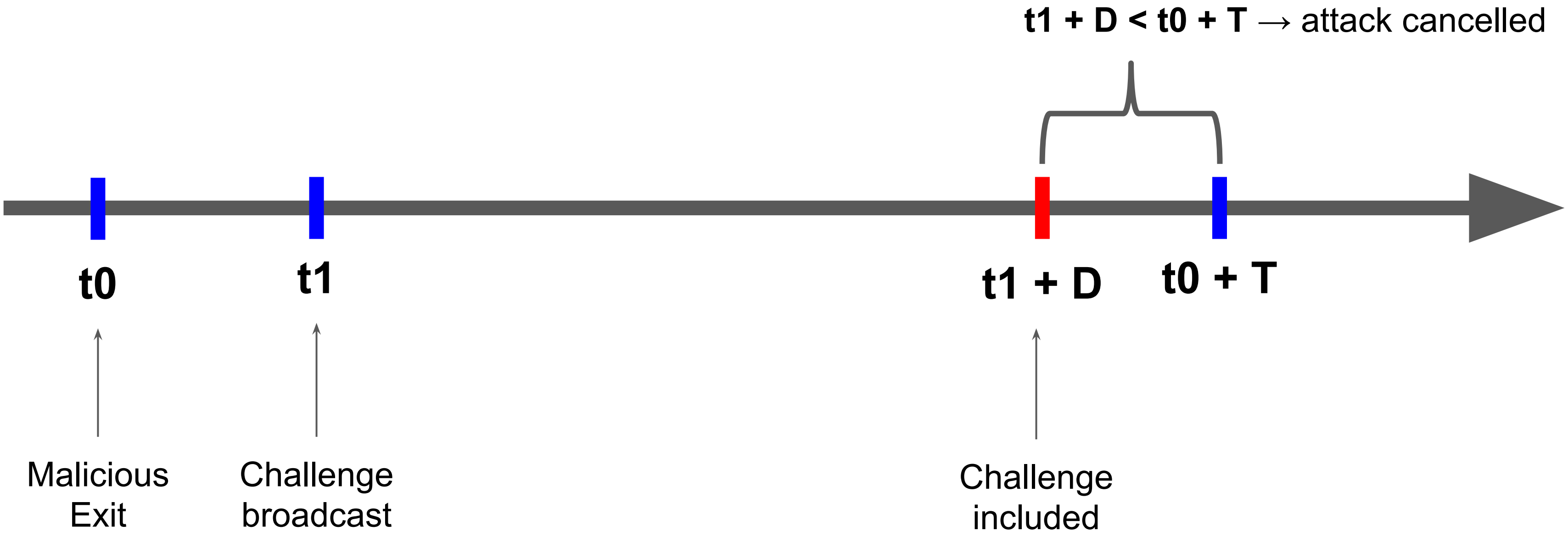
- **liveness (somebody must challenge)**
- **expected reward of attacker <=0**

*L2 games are implemented as deferred optimists: *https://medium.com/@decanus/optimistic-contracts-fb75efa7ca84*

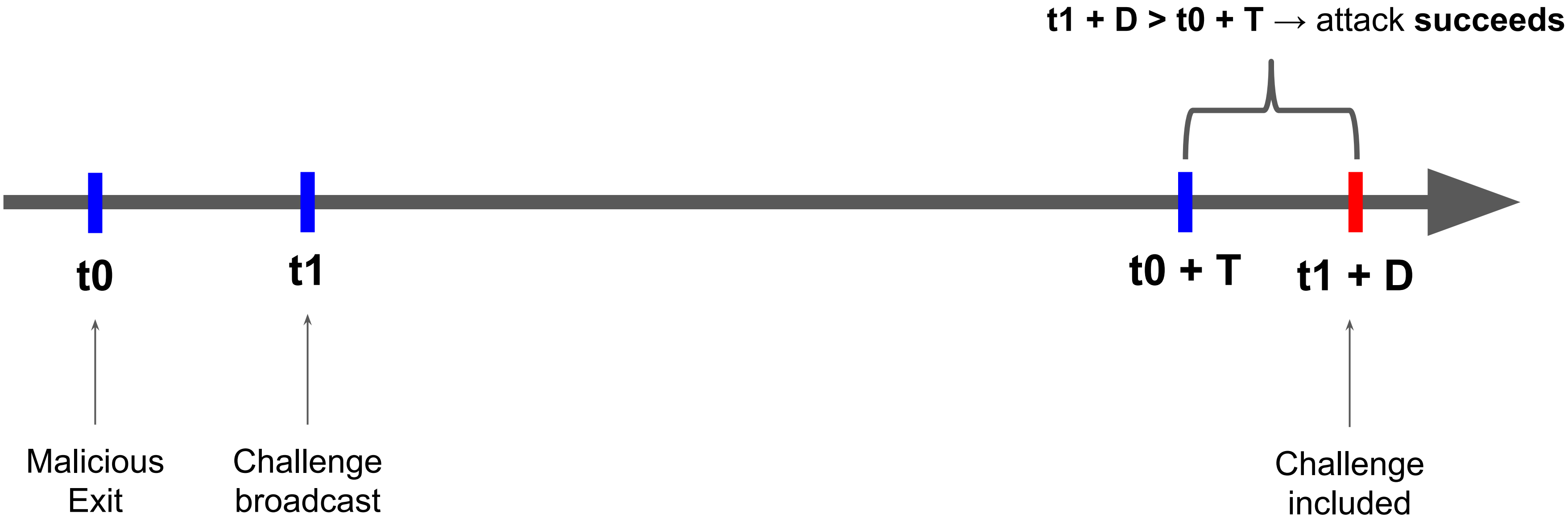
Secure iff challenge included before t0 + T



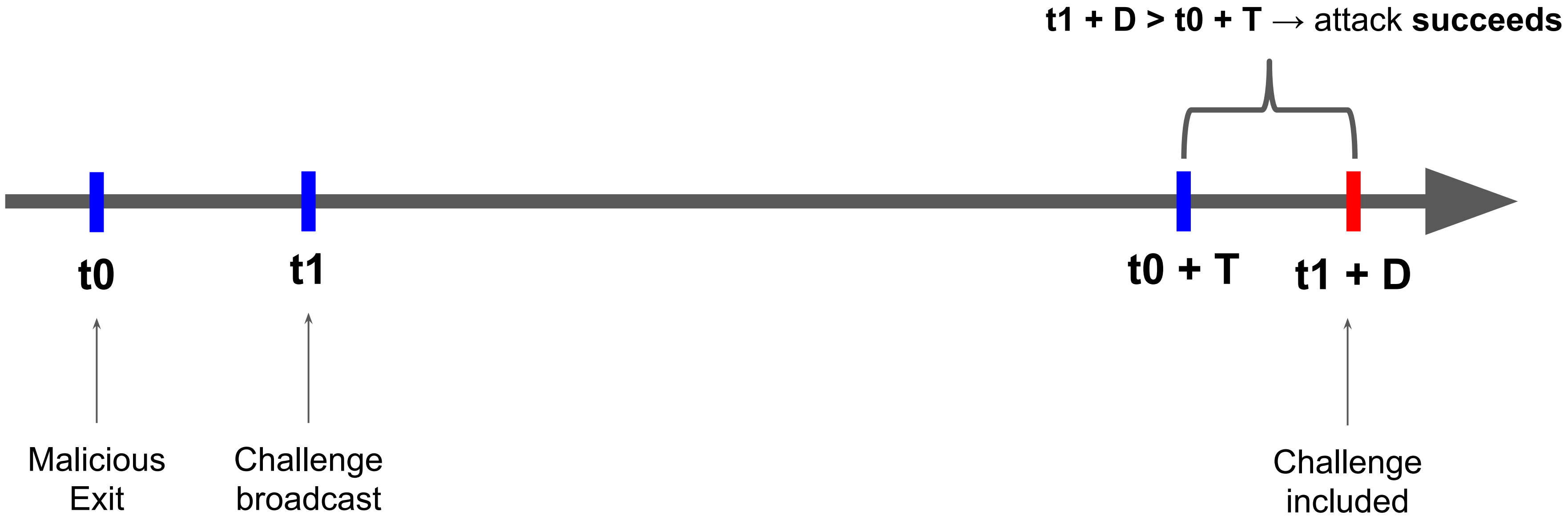
Secure iff challenge included before t0 + T



Insecure iff no challenge included before t0 + T



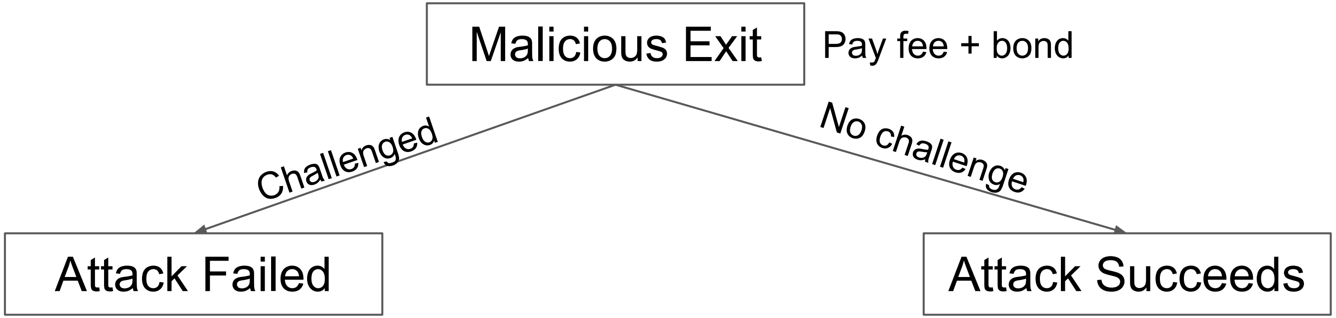
Insecure iff no challenge included before t0 + T



Safety condition: D <= T + $\boxed{\text{t0 - t1}}$

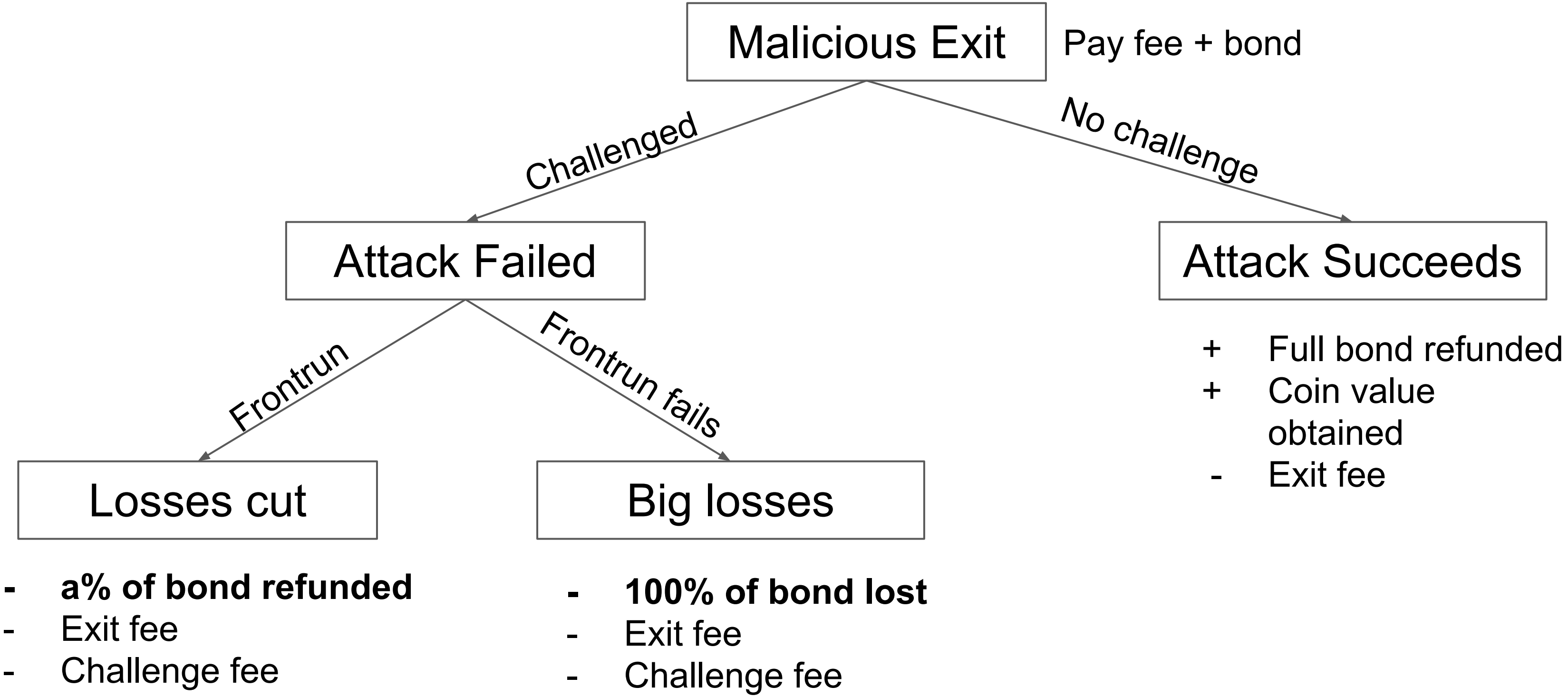
Liveness of observers

Attacker Decision Flow



- + Full bond refunded
- + Coin value obtained
- - Exit fee

Attacker Decision Flow



Malicious Exit

Pay fee + bond

Challenged

No challenge

Attack Failed

Attack Succeeds

+ Full bond refunded
+ Coin value obtained
- Exit fee

Frontrun

Frontrun fails

Losses cut

- **a% of bond refunded**
- Exit fee
- Challenge fee

Big losses

- **100% of bond lost**
- Exit fee
- Challenge fee

Incentive Compatibility of the Exit Game

$$E(R) = P(\overline{C})v \qquad\qquad \leq 0$$

No challenges = success:

- ↑ onchain congestion / censorship
- ↑ block withholding
- ↓ liveness of participants
- ↓ **challenge period *T***

Large T = Secure but bad UX!

Incentive Compatibility of the Exit Game

$$E(R) = P(\overline{C})v - \underbrace{[gas + P(C) * bond]}_{cost\ to\ attack} \qquad \leq 0$$

No challenges = success:

- ↑ onchain congestion / censorship
- ↑ block withholding
- ↓ liveness of participants
- ↓ **challenge period *T***

Large T = Secure but bad UX!

Cost to Attack =

- Tx fees (constant)
- **Fidelity Bond**
  (goes to challenger)

Incentive Compatibility of the Exit Game

$$E(R) = P(\overline{C})v - \underbrace{[gas + P(C) * bond]}_{cost\ to\ attack} + \underbrace{P(C)P(F \mid C) * bond}_{reward\ from\ frontrunning} \leq 0$$

No challenges = success:

- ↑ onchain congestion / censorship
- ↑ block withholding
- ↓ liveness of participants
- ↓ **challenge period *T***

Large T = Secure but bad UX!

Cost to Attack =

- Tx fees (constant)
- **Fidelity Bond** (goes to challenger)

Frontrunning removes bond from cost if successful

$$P(F \mid \overline{C}) = 0$$

Attacker won’t frontrun if nobody challenged

Incentive Compatibility of the Exit Game

$$E(R) = P(\overline{C})v - \underbrace{[gas + P(C) * bond]}_{cost\ to\ attack} + \underbrace{\alpha P(C)P(F \mid C) * bond}_{reward\ from\ frontrunning} \leq 0$$

No challenges = success:

- ↑ onchain congestion / censorship
- ↑ block withholding
- ↓ liveness of participants
- ↓ **challenge period *T***

Large T = Secure but bad UX!

Cost to Attack =

- Tx fees (constant)
- **Fidelity Bond**
(goes to challenger)

$$P(F \mid \overline{C}) = 0$$

Attacker won't frontrun if nobody challenged

Frontrunning removes bond from cost if successful

↓

Burn part of the bond.