Pinkcoin (2017)

Preliminary Security Review

_MiW, 2017-08-19

```
"'Tis the Pink of the Mode, to marry at first Sight: - And some, indeed, marry without any Sight at all."
 -- Kensington-Gardens; or, the pretenders: A Comedy, John Leigh
```

```
Disclaimer: This document is the opinion of the author at the time of writing.
As this space changes rapidly, it may not match the current market or code conditions at the time of reading.
This is not investment advice, and should not taken as such.
At the time of writing, the author is in control of 0 PINK.
```

Wha?

Pinkcoin is a new (2017) hybrid proof-of-stake (PoS) proof-of-work (PoW) proof-of-flash-stake (PoFS) cryptocurrency, based on the Genstake cryptocurrency .

The project was relaunched with a new development team in 2017 with a new Proof Of Work and cryptoeconomic parameters. It did not share existing transaction history with Pinkcoin1 (OLDPINK).

Pinkcoin was originally launched in 2014 as a X11 PoW/PoS coin. At the time, X11 was seen as way of providing 'ASIC resistance' by employing multiple hashing algorithms. With the lens of 2017, this ultimately was not successful. The (2017) PoW function is 'scrypt' (litecoin, et al).

The new team ran a coin-swap for the legacy Pinkcoin1 holders. The coins from the old chain are sent to burn addresses.
These OLDPINK coins are burned in OLDPINK addreses:

```
P8x19kCormutUqTJrXeMyXNhfAqRoVzH1R
PUxNb9zLJpBtAVXNYyikGaX6AyqSeTmD7G
PN1KBurnedCoinsHereForeverxxvKBhL8
```

It is believed that at least one of these may be an exchange (cold?) wallet that refused to spend to an unspendable address.

The original release (2014) had the following cryptoeconomic parameters:

```
Algorithm: X11 POW/POS
Total coin: Was: 500,000,000  At time of swap: ~380,000,000
Block reward: 25000
POW last: 20000 - 7 days POW only(done)
POS generate after 10000 block
Block time: 30 seconds
```

```
POS Min age: 8 hours
POS Max age: unlimited
Confirmations on Transactions: 10
Maturity: 500
Stake interest: 1%/year
No Premine
```

The new chain has the following cryptoeconomic parameters:

```
Algorithm: Scrypt
Maximum coin: 500,000,000
POW and POS hybrid forever
Target Time between PoW Blocks:  2 Minutes
Target Time between PoS Blocks: 6 Minutes
Target Time between FlashStaking Blocks: 1 Minute
POS Min Age: 1 hour
POS Max Age: 30 days
Proof of Work reward starts at block: 17000
Proof Stake reward starts at block: 16240
Time between new PoS modifiers : 5 mins
PoS Reward: 150 PINK per Flash; 100 PINK
POW Reward: 50 PINK per Block
PoS/PoW decay following PoW curve: reward / 1+floor( year_of_chain / 2)

Flash Stake Hours
nHour1 = 7am PST
nHour2 =12pm PST
nHour3 = 5pm PST
nHour4 = 10pm PST
```

The new chain was launched on 2017-03-08 02:30:23

364800000 PINK were Premined in the genesis block .

These coins are controlled by the development team in hot and cold addresses.

As of 2017-08-19 320, The cold swap wallet contained ~30,000,000 PINK.
195,430.52680731 coins had be swapped from the old chain. Thus a claim ratio of ~88% was achieved within ~6 months.

(This would be considered high for a coinswap in this space).

New Origins

Genstake was a fork of Jumbucks . Jumbucks was a fork of ShadowCoin forked from Blackcoin .
These are in turn derived from Novacoin and PPCoin/Peercoin

Pinkcoin introduces the novel Flash Staking, which alters the rate and reward of the staking process. The staking reward model encourages wallets to be left online, further strengthening the number of block verifying nodes.

Pinkcoin branding is based around tipping and charity, and stresses inclusivitity. The project also runs the Donte4Life system, which offer donors a perpetual staked donations to charity.

Change in Stake Emission Curve

The new stake reward algorithm is:

Block Reward = Base Reward * 1/floor(1+blockchain_year/2)

Which results in the following reward schedule:

Year	PoW	PoS	FpoS
0	50.00	100.00	150.00
1	50.00	100.00	150.00
2	25.00	50.00	75.00
3	25.00	50.00	75.00
4	16.67	33.33	50.00
5	16.67	33.33	50.00
6	12.50	25.00	37.50
7	12.50	25.00	37.50
8	10.00	20.00	30.00
9	10.00	20.00	30.00
10	8.33	16.67	25.00
11	8.33	16.67	25.00
12	7.14	14.29	21.43
13	7.14	14.29	21.43
14	6.25	12.50	18.75
15	6.25	12.50	18.75
16	5.56	11.11	16.67

Year	PoW	PoS	FpoS
17	5.56	11.11	16.67
18	5.00	10.00	15.00
19	5.00	10.00	15.00
20	4.55	9.09	13.64

And the resultant total outstanding coin per year

Year	Actual	Intended
0	398380000	398380000
1	431960000	431960000
2	448750000	448750000
3	465540000	465540000
4	476733333.333333	473935000
5	487926666.666667	482330000
6	496321666.666667	486527500
7	504716666.666667	490725000
8	511432666.666667	492823750
9	518148666.666667	494922500
10	523745333.333333	495971875
11	529342000	497021250
12	534139142.857143	497545937.5
13	538936285.714286	498070625
14	543133785.714286	498332968.75
15	547331285.714286	498595312.5
16	551062396.825397	498726484.375
17	554793507.936508	498857656.25
18	558151507.936508	498923242.1875

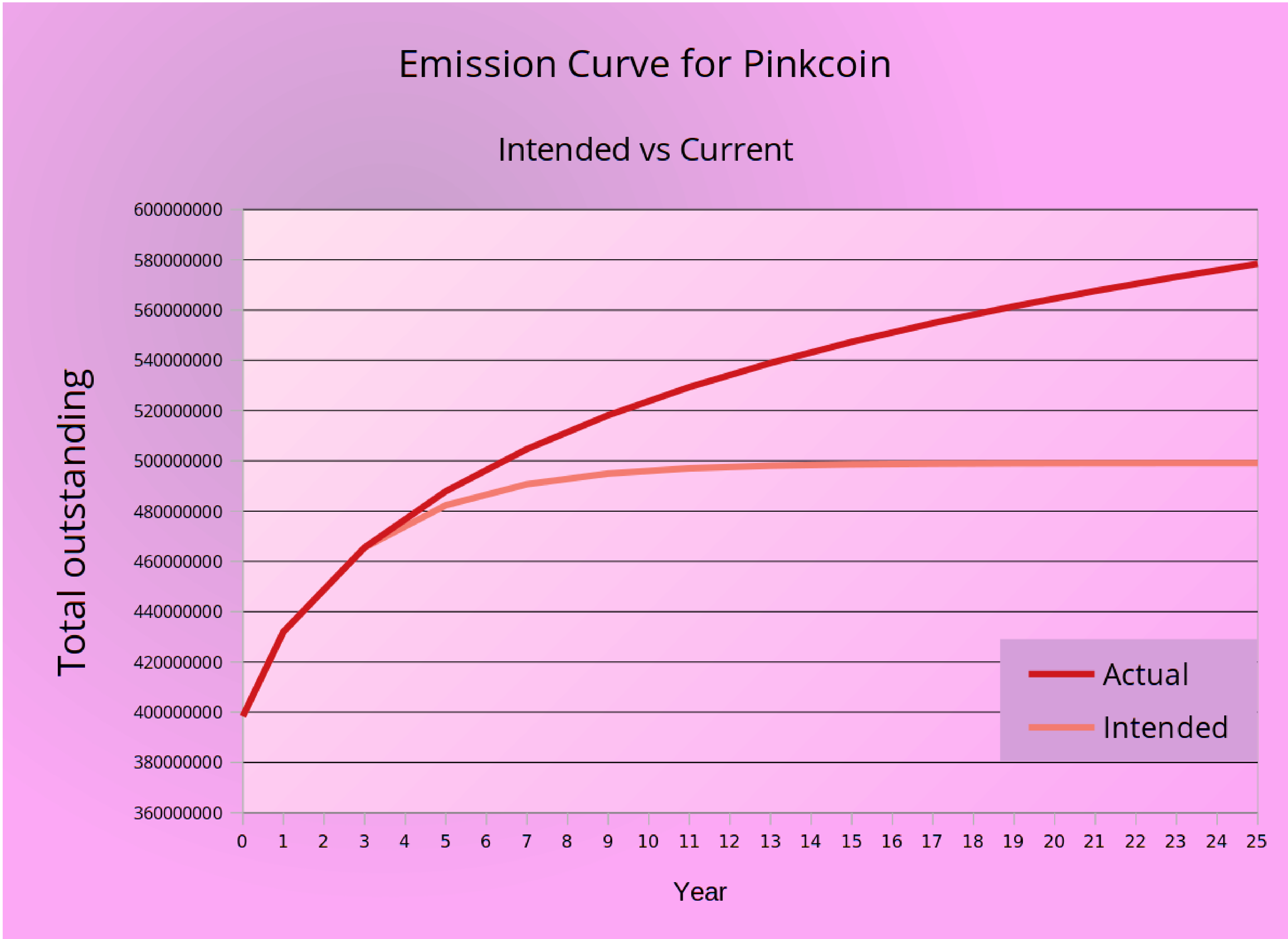
Year	Actual	Intended
19	561509507.936508	498988828.125
20	564562235.209235	499021621.09375
21	567614962.481963	499054414.0625
22	570413295.815296	499070810.546875
23	573211629.148629	499087207.03125
24	575794706.071706	499095405.273438
25	578377782.994783	499103603.515625

```
2 mins / PoW block * 50
6 mins / PoS block * 100 * (20/24 hours)
1 min / FPoS block * 150 * (4/24 hours)

Reward 1/2 PoW Blocks a Min providing 50 = 1/2 * 50 * 1440 = 36000 PINK / day (720 blocks a day)
Reward 1/6*5/6 PoS Blocks a Min providing 100 = 1/6 * 5/6 * 100 * 1440 = 20000 PINK / day (200 blocks / day)
Reward 1*1/6 FPoS Block a Min providing 150 = 1/6 * 150 * 1440 = 36000 PINK / day (240 blocks / day)

Total Reward per day: 36000 + 20000 + 36000 = 92000
Projected Blocks / day: 720 + 200 + 240 = 1160
Average reward / block = 79.31

Calculated average coin emission over the last 100 blocks as of 2017-08-19: 87348
```



The intention of the coin is to have a Base Reward that halves every 2 years, rather than this divergent harmonic series. This is currently a bug that must be resolved before the block reward changes, to maintain consensus.

The author proposed Reward = BaseReward / 2^floor(blockchain_year/2)

Developer comment on change of emission regarding not using coin age for reward (interest)

"Something to consider with the fixed rewards vs. interest % based rewards model.

The number of coins you successfully mint is proportional to your weight vs. network weight, and achieving your optimal weight requires an investment of 30 days of time.

So, say I buy a million pink. Among other things, in order to achieve my optimal weight, and thus mint the most blocks possible for the number of coins I have, I have to hold them in my wallet for 30 days. If I am staking those coins, they are removed from circulation. In this scenario, three things happen:

1. 1m coins are purchased and remove from the market, elevating the value of coins available for trade.
2. 1m coins gather weight on the network over 30 days, ultimately increasing the overall network weight by 30m, proportionally reducing the number of coins everyone else mints.
3. Moving those 1m coins back into circulation comes at the expense of the time invested holding those coins, and their potential rewards through the process of staking. This helps add stability to the market.

If someone with a large number of coins does decide to stop staking and dump their coins, the entire network of remaining stakers benefits from the reduced network weight. A reduced network weight creates an incentive to invest and move coins off the exchange for staking, while people that have staked the whole time see some benefit for at least 30 days if someone else decides to move coins into a staking position.

In practice, we've all seen these waves, as the average network weight (with consideration to people gaming flashstaking periods) seems to follow a receding pattern followed by growth. So 400m to 700m to 500m to 1b to 800m to 1.4b to 1b to 2b. These numbers are significant, as 2b weight means that the equivalent of 67m coins with max weight are actively staking, and in turn, can be assumed off the market.

Something else is that Polo requires 40 confirmations for PInk - so moving coins from a wallet to the largest exchange takes about an hour, or a little over 30 mins during a 'flash period', which also helps reduce the incentive to panic sell."

Compiling Pinkcoin

Source was obtained from github

The depends openssl and bdb4 had beeen previously compiled for other bitcoin-like wallets, and were included as environment variables. As older bitcoin codebase (now migrated to libsecp256k1) required libssl API 1.0, we must include a manual build of it as the application will no longer compile on OpenSSL 1.1

To build the console daemon:

```
git clone https://github.com/PinkDev/Pink2
cd Pink2
cd src
export BDB_LIB_PATH=${HOME}/Development/db4/lib
export BDB_INCLUDE_PATH=${HOME}/Development/db4/include
export OPENSSL_LIB_PATH=${HOME}/Development/openssl/1.0.2l/lib
export OPENSSL_INCLUDE_PATH=${HOME}/Development/openssl/1.0.2l/include
make -f makefile.unix
```

To build the GUI

```
qmake  BDB_LIB_PATH=${HOME}/Development/db4/lib BDB_INCLUDE_PATH=${HOME}/Development/db4/include OPENSSL_LIB_PATH=${HOME}/Development/openssl/1.0.2l/li
make
```

The D4L

The donate for life stakefund exists as a sinkhole for the unclaimed premined coins. The D4L wallet must be online 24/7 with its private keys hot in memory.

The D4L key material must be online for valid stake blocks to be generated. These work by making special stake (or flashstake) blocks that claim a D4L Unspent Transaction Outputs (UTXO), and

Key Material

If this address was a multi-sig, implemented as a Pay-to-Script-Hash (P2SH) tx, it would require a valid multi-signature script in order to claim.

This reduces the problem to either a hot claim script or hot private key, both acting are barer tokens to either spend or stake the balance. Either way, it is a single point of vulnerability, in which a future presumably large charity stake could be compromised if this key is disclosed.

Key disclosure would allow the attacker to claim and spend the D4L UTXO.
This could lead to extreme reputational and economic damage.

Mitgations

The developers have stated that the D4L address should be unspendable, and only used for staking. This could further be enforced by consensus rules that enforce:

1. No D4L UTXO as inputs in a standard pay-to-pubkey-hash (P2PKH) (blacklist inputs)
2. Explicit list of valid possible stake coinbase tx output public keys (whitelist outputs)

If 1. was implemented, it would mean an attacker who had compromised the D4L keys could not spent the funds, however it would be a race to spend the staked funds.

If 2. was implemented, at best, the attacker could only force a particular whitelisted address to recieve the stake. This is unlikely to cause economic damage until a Hark Fork issued to regain control of those funds.

Further discussions with developers

Further discussion with the development team explained that the idea for a user controlled permastake/stake4l would be that users could create their own dynamic stake4l address that behaves like the central d4l. This could be done via the user wallet, with users in full control of the stake output destination.

This would enable users to 'be their own charity', and decentralize the coin distribution and increase network security with more staking full nodes.
Decentralized Autonomous Charities!

The team explained that an ultimate goal would be that the central d4l private keys could be published and would stake to a separate database. This would enable the users to stake the coins on behalf of the d4l distribution mechanism. This would fully decentralize the core charity function of the project.

Presently, the d4l keys are controlled by the development team via the a proxy system to direct the funds. There is a plan to whitelist these proxy addresses as a way of enforcing 2. The key compromise scenario had been considered by the development team, and were working on a key rotation disaster recovery solution.

It was highlighted that Sabotage and lack of consensus enforcement that the D4L stake could not be burned were current problems with a general whitelist/blacklist solution as of now. Sabotage attack would maliciously burning all coin age by staking the entire UTXO set; This would reset the continuous emission of stake suitable for donation. The current lack of consensus differentiation between stake-mint/principal could permit spending the stake to the whitelist address.

In order to mitigate sending the stake to the whitelist, the author suggests considering making the stake coinbase tx split the stake payout between two UTXO for mint and principal. Some tag on the principal transaction could prevent this from being included in other tx inputs.

There was ongoing research into same-address multi-instance stake behavior to determine decentralized D4L staking. This could be an interesting area, and may result in new cryptoeconomic techniques. One idea could be 'decentralized single-computation by stake' smart contract execution; decentralized run once verify everywhere!

Coin Distribution

```
This is based on open-source research, conversations and assumption.
It may not be correct.
```

Sourced from https://chainz.cryptoid.info/pink/#!rich on 2017-08-19

~95 % (~358M) of the outstanding coins are held in the top 100 addresses.
~71 % (~270M) are controlled by the top 10 addresses.

Rank	Address	Balance	Possible Description (could be incorrect)	Percent	Total Outstanding	Cumulative Percent of Outstanding
1	2MPDZ6Ke2gNyd61RUY3CH8YYFkLiyytzZz	157839187.5	Exchange Cold Wallet (Poloniex?) [Not Staking]	41.78%	157839187.5	41.78%
2	2Ki78CrqJMZBPP8y4ShhstMJantscKUe24	35966142.54	Unknown Cold Wallet (Bitrex?) [Not Staking]	9.52%	193805330.04	51.31%
3	2TMJ2bzjHqXomc7tL4MHNu2tmv5VXqByDS	30000000	Swap Cold Wallet [Not Staking]	7.94%	223805330.04	59.25%
4	2HSdkiURYyUBBYXg8bGihXgVXnGhn3ysRM	11521514.54	Exchange Hot Wallet (Poloniex?) [Not Staking]	3.05%	235326844.58	62.30%
5	2aMVkzfjCPDcwsKZi5GJGCB9mCBFZ4quSL	8469502.11	Unknown/Developers/Was staking but offline	2.24%	243796346.69	64.54%
6	2MCDV28ESwgfmYmN5NMxqvApe3EDqm4srw	6264441.44	Unknown/Developers/ExchangeHot?	1.66%	250060788.13	66.20%
7	2FSQPekXKUvJGWuyYoWvfG3Ej9SzZhTGfr	6015956.31	Unknown/Developers/ExchangeHot?	1.59%	256076744.44	67.79%
8	2Me1yE7YPaBPTMJDhdXTAYzgWpmiY6su1P	5303253.7	Unknown/Exchange Deposit Address? [Not Staking]	1.40%	261379998.14	69.19%
9	2PqpqcRqrYaiUBHKgv9svcJiHsze2JifDz	5278527.1	Unknown/Developers/ExchangeHot?	1.40%	266658525.24	70.59%
10	2VnWfAJK2Q2UNoC6PSc17BZCbnoNwtD6zM	4229425.05	Unknown/Developers/ExchangeHot?	1.12%	270887950.29	71.71%
11	2UhwLhxduAMGuYYp6wLz71XE7D3zaMeVso	3942610.01	Unknown/Developers/Cold? [Not Staking]	1.04%	274830560.3	72.76%

Rank	Address	Balance	Possible Description (could be incorrect)	Percent	Total Outstanding	Cumulative Percent of Outstanding
12	2P6EnyvzMX9Q6oGK4t7XsboBNsCfxyojMq	3118186.23	Unknown/Developers/ExchangeHot?	0.83%	277948746.53	73.58%
13	2KGBQA4ZJbmLNszE3Mn4JnwJbue7MBubKt	3003511.36	Unknown/Developers/ExchangeHot?	0.80%	280952257.89	74.38%
14	2GCaWXMqeWnn81ppJBD6gwye9vAG4ADAZR	3000374	Staking Wallet sending reward elsewhere	0.79%	283952631.89	75.17%
15	2TXTSNkEoY17nerddwDsQTetAVcUsnXWQ9	2852074.3	Unknown/Developers/Staking wallet?	0.76%	286804706.19	75.93%
16	2EmGnWWbSBSxR3gKF7coSKC69Rh2k1uaef	2121540.83	Unknown/Developers/Staking wallet?	0.56%	288926247.02	76.49%
17	2RPfe1EyEMrK6yW87G71Yf6AN6PZvprGNT	2039694.34	Unknown/Developers/Staking wallet?	0.54%	290965941.36	77.03%
18	2FBQZTwaUnqW1mDGrnsxWUwSZ8zGJdPNrT	1996678.81	Unknown/Developers/Staking wallet?	0.53%	292962620.17	77.56%
19	2WDDSjAwgB54s5YBtzaxvNuXdCxxtA54iC	1962673.6	Unknown/Developers/Staking wallet?	0.52%	294925293.77	78.07%
20	2KNuViLrHBhMrHyjmmaJ1zq2ZZz6kBZTdm	1918781.98	Unknown/Developers/Staking wallet?	0.51%	296844075.75	78.58%
21	2R1VUrf44WdDY85nXcSeBk7h1iTdY9Pe1F	1872147.81	Staking Wallet sending reward elsewhere	0.50%	298716223.56	79.08%
22	2VgnAGAbk9GsLWKKXmLE4cULcSJXQeMnrz	1637969.02	Unknown/Developers/Staking wallet?	0.43%	300354192.58	79.51%
23	2Zjrn3NG6WoGAY4iqVy81FaqBdwtSvfa5F	1637525.56	Staking Wallet with larger deposits (Exchange Hot?)	0.43%	301991718.14	79.95%
24	2RPGW1ioN4xYfaPDYrUsntX7MA6utnrQo5	1625653.1	Unknown/Developers/Staking wallet?	0.43%	303617371.24	80.38%
25	2DQXX1rhFNdFQaTqariSqwXGnWJ2M3LNQC	1590934.88	Staking Wallet with smaller deposits (Miner?)	0.42%	305208306.12	80.80%
26	2M46Pybw6xnESQRB8ra3wqFmsRuC5gtRpc	1553751.44	Unknown/Developers/Cold? [Not Staking]	0.41%	306762057.56	81.21%
27	2U3qaz4766qCLUuYrW6HZDz1cGftFVN8uK	1522302.92	Staking Wallet with larger deposits (Exchange Hot?)	0.40%	308284360.48	81.61%
28	2LNjv7nh22WWZPgzpLgihLqtVoh4UBwzyw	1501183.11	Staking Wallet sending reward elsewhere	0.40%	309785543.59	82.01%

Rank	Address	Balance	Possible Description (could be incorrect)	Percent	Total Outstanding	Cumulative Percent of Outstanding
29	2S3rHYngLmRgGaHiiDecUMaZ5AjHqV1bAC	1369313.28	Charity Fund (D4L)	0.36%	311154856.87	82.37%
30	2ZYti9mPjQndCiqRZgP9JrKksparzeLzu4	1273073.07	Unknown/Developers/Miners?	0.34%	312427929.94	82.71%
31	2QJmgE5tw5XTqZnCpYcLhTqVEDd1k25exE	1269312.44	Rain Cloud	0.34%	313697242.38	83.04%
32	2UbAdXbZiphAhqqBP2bnXMv31DMZdm51SL	1269066.86	Marking Fund (D4L)	0.34%	314966309.24	83.38%
33	2UtMZ5DLocTfTi6eLtcPATHpPn5tc1YzGm	1268036.18	Education Fund (D4L)	0.34%	316234345.42	83.72%
34	2TwEnncttTb2bJk6hHi1JGgGeT4u78grSN	1267704.44	Development Fund (D4L)	0.34%	317502049.86	84.05%
35	2ZysRrYxRGmQhH2cgScqwLoVobB9BTmmvC	1267167.48	Elder Tree	0.34%	318769217.34	84.39%
36	2Gbp17xubGBQ8aGWAi4PRryq9f9UvVmkFd	1267162.82	Acorns	0.34%	320036380.16	84.72%
37	2VQce1omBJenvJnHZyXvacwzgsQq9hG2nj	1262957.6	Staking Wallet with smaller deposits (Miner?)	0.33%	321299337.76	85.06%
38	2PykknVcPtokED9WHo829XLyApj9ymfjg6	1262935.44	Staking Wallet with smaller deposits (Miner?)	0.33%	322562273.2	85.39%
39	2JKP5fqjCaGHT55yN9kZUMFFiMk4npaGs8	1228404	Staking Wallet with smaller deposits (Miner?)	0.33%	323790677.2	85.72%
40	2KsPNoUPgmVhBHUbEqyUowzhJLXbTkqZsX	1175930.68	Staking Wallet sending reward elsewhere (Exchange?)	0.31%	324966607.88	86.03%
41	2UQPr99ppBpzJjjzTXfiAMz5DRmGHx1fiq	1173785.59	Staking Wallet with smaller deposits (Miner?)	0.31%	326140393.47	86.34%
42	2aj45qsESX5HhYBcU9MP6o5uF8p64VbdSW	1117770.06	Occasionally online staking wallet (mostly cold)	0.30%	327258163.53	86.63%
43	2L9JgpFsFddp3Mif7zoXuvz37X1oDrTckw	1115320.22	Staking Wallet with larger deposits (Exchange Hot?)	0.30%	328373483.75	86.93%
44	2aQazSoe7XVSWKKKMkET3zpxk4fURReSDp	1100000	Cold Wallet [Not Staking]	0.29%	329473483.75	87.22%
45	2NQysQSyJ3QCNR1jHYYdAaPuRnSgciHKe2	1081637.41	Staking Wallet with smaller deposits (Miner?)	0.29%	330555121.16	87.51%
46	2TZk1x8xinWHZHguCS29dsJYBp6eHSwA7D	1078212.34	Staking Wallet with smaller deposits (Miner?)	0.29%	331633333.5	87.79%
47	2UjFqcmMdTbNEqEX87BkcmEFrNiz4vwrbc	1078054.07	Staking Wallet with smaller deposits (Miner?)	0.29%	332711387.57	88.08%

Rank	Address	Balance	Possible Description (could be incorrect)	Percent	Total Outstanding	Cumulative Percent of Outstanding
48	2bvhNDFey5sCyv7AGc1chD7VgUvG6iDTpW	1032303.9	Online staking with larger deposits (Exchange?)	0.27%	333743691.47	88.35%
49	2ZuUVj58hikWxmZPy4Bzk97oVV6nMThWLq	1002721.91	Cold Wallet with single stake [Not staking]	0.27%	334746413.38	88.62%
50	2D4FMbNFU3AjRgE3W8RsPS1wAJpW25mDn9	1000587.95	Random Fund (D4L)	0.26%	335747001.33	88.88%
51	2KBM9vqtGGGB4BTbHY7BoD8wHkzNzZLcaC	1000000	Cold Wallet? [Not Staking]	0.26%	336747001.33	89.15%

Observations on Diff genstake & pinkcoin

```
diff -Naur -X exclude ../Pink2 ../genstake > genstake-diff.txt
```

- Testnet alert key is same as genstake (recommend rotate testnet key)
- Recommendation to upgrade to OpenSSL 1.1+ API for future compatibility with os qt5 packages
- https://github.com/PinkDev/Pink2/blob/master/src/bitcoinrpc.cpp#L1394
  Commented function, should use == not =
- Genstake had a wait of 10000 blocks before wallets could stake. Pinkcoin has removed this and can stake immediately. Removes the 10000 block waiting stake time checkpoint adjustment. Pinkcoin required 17000 blocks before there was a mining reward. Block 17000 occurred 2017-03-25 05:31:49, which meant that during this time there were 0 new coins created by mining.
  In this 17 day period, 35,800 PINK were staked from transactions originally generated from the premine, negligible given the total coin count in circulation at that time.

Use of BDB4/BDB5

- doc/readme-qt.rst makes reference to Berkely DB issue on debian.
  States that debian binaries may have been shipped linked to BDB5.

It is recommended that all bitcoin derivatives not to link against BDB5 for wallet compat. This is likely a legacy comment as most bitcoin-like code explicitly will not use BDB5.

It is encouraged to not ship static DB5 linked binaries as they can break user wallet compat. It is worth considering a new wallet format.

Interesting Code Snippits

Mining reward schedule - main.cpp:980

```
if (nHeight == 1)
        nSubsidy = 364800000 * COIN; // Pinkcoin Coinbase.

    if (nHeight >= 17000)
        nSubsidy = 50 * COIN / (1 + (nHeight / nHalvingPoint / YEARLY_BLOCKCOUNT));
```

Stake reward schedule - main.cpp:997

```
int64_t GetProofOfStakeReward(int64_t nCoinAge, int64_t nFees, int nHeight, unsigned int nTime)
{
    int64_t nSubsidy = 0;

    if (nHeight >= 16240)
    {
        if (IsFlashStakeReward(nTime))
        {
            nSubsidy = 150 * COIN / (1 + (nHeight / nHalvingPoint / YEARLY_BLOCKCOUNT));
            printf("\n\nIsFlashStake\n\n");
        } else {
            nSubsidy = 100 * COIN / (1 + (nHeight / nHalvingPoint / YEARLY_BLOCKCOUNT));
            printf("\n\nIs NOT FlashStake\n\n");
        }

    }

    if (fDebug && GetBoolArg("-printcreation"))
        printf("GetProofOfStakeReward(): create=%s nCoinAge=%d\n", FormatMoney(nSubsidy).c_str(), nCoinAge);

    return nSubsidy + nFees;
}
```

The premine for the genesis block - main.cpp:985

```
    if (nHeight == 1)
        nSubsidy = 364800000 * COIN; // Pinkcoin Coinbase.
```

Risks

- OLDPINK Resurrection

  - Very difficult with a single large UTXO, however the unlimited POS validity time in OLDPINK could generate a valid block in the future. It would likely take significant time for this chain to regain validity.
  - **Severity** : Medium
  - **Likelyhood** : Highly unlikely
  - Development team reply: "those coins can't be used to resurrect the chain. Old pink used a 510 block maturity period. Even if they could get them to stake, they'd stake exactly once, and then be forever stuck in maturity. If they tried to send any portion of the coins, they would need other coins to actually stake a block to complete that send. The staking process itself was bugged as old and/or large numbers of coins would never stake properly due to the staking function generating numbers in excess of the capacity afforded by uint64. In order to make it work, they'd either have to fork it or run the network on their own, the old chain itself is almost impossible to sync to - a third of the chain is orphans, and that's on top of the > 3 million blocks. Running old pink requires ~2gb of memory, and an average server is only capable of processing a few dozen blocks a second as the block count becomes excessively large. Add that there's only a couple of nodes still live on the network at all, and that only a centralized approach could revive it, and those coins would be known to be controlled by /the exchange/. I don't see why anyone would pick up old pink. It died because we literally couldn't get another block out of it with our own wallets, and there's only been a couple of blocks since."

- Compromise of D4L keys

  - Single central online private key could be future large securing network stake
  - **Severity** : High
  - **Likelyhood** : Very Low
  - Severity can be reduced by future consensus enforcing rules such as blacklist/whitelisting of inputs/outputs. Further mitigation are discussed around decentralization in D4L section.
  - Development team reply: "At the moment we're using a proxy address system to direct the funds - these in turn will be what gets whitelisted for stake coinbase tx's. So each D4L address is paired with an address that we control, and the coins in those addresses are directed to their ultimate destination. Using this pair scheme means that a malicious entity could not change where the staked funds themselves are directed. I'm toying with a few ideas for how to change them if one happens to become compromised, but that's how it's being handled at this point."

- Large non-staking cold wallet

  - The address with the largest balance is believed to be a major stake cold wallet. As these keys are offline they will not generate stake blocks.
    If a large amount of coin is offline for the life of the coin, it may reduce the number of staked blocks.
    This may be counterbalanced by stake emission not being tied to the age of the coin directly.
  - **Severity** : Low
  - **Likelyhood** : Certain
  - Encourage decentralization of exchange cold wallet by requesting users be custodian of funds. Find further incentive beyond staking. Increase community size to offset.

- MAX_MONEY cap (500,000,000) is not enforced in the emission schedule

  - At some point in the future, this will need to be enforced to prevent inflation.
  - Currently the code base enforces MAX_MONEY validity checks on RPC commands as well as transaction validity, but not in emission.
  - Plenty of time to implement checks.
  - **Severity** : Low
  - **Likelyhood** : Currently certain, can be mitigated in the future to impossible
  - 1/n is a divergent series and was implemented in error.
  - Development team reply: "so far we're way under budget for the number of blocks, I don't think it's actually possible to hit 500m anymore. Dividing the number of coins minted since genesis into the expected number of blocks per day produces an average daily coins generated of 87516.13 - which is significantly less than the predicted 92k/day. If that average holds out we cap at 492,573,551."
  - Development team reply: "Next update will have the fixed halving code. People will have 3 1/2 years to update before the soft fork when their stakes wont be accepted by the network."

Conclusions and Recommendations

- https for all websites. Use wildcard for all virtual hosts.
  - Lets Encrypt wildcard Certificates will be available in Jan 2018
  - Can use per vhost LE Cert until wildcard is gratis; Or purchase a wildcard in interim.
- Fix Harmonic Divergent Emission for PoW and PoS
  - Suggested Reward = BaseReward / 2^floor(blockchain_year/2)
- Improve test coverage of codebase
- Prioritize code documentation. Bitcoin was always bad for this!
- Updated project documentation in repo. Up to date Readme.md
- Rotate Testnet alert key from genstake testnet key
  - Key reused between coins
- Migrate from OpenSSL 1.0 API for compat with modern system libraries
- Implement libsecp256k1 for perf
- Publish confirmation (or statement explaining situation) about 'unburned'
- Publish research on single-wallet multiple-instance stake behavior
- Publish key compromise Disaster Recovery plan until such time decentralized autonomous charities are live
- Consider moving away from BDB for wallet persistence
- Evaluate language migration