The Bitcoin White Paper Visualized

Understanding Cryptocurrency's Big Bang

The Bitcoin White Paper by "Satoshi Nakamoto" turns ten years old this month. Today, arguments rage about manic speculation, "dark web" sales, cryptocurrency's carbon footprint, and warring technical standards. But before Bitcoin became a popular phenomenon, it was an **idea**—a concept greater than any ticker symbol: **electronic cash for the entire world**. This idea still exists, and it's a **fascinating** one that too few understand. I hope this helps.

— Scott McCloud, November 2018

Bitcoin: A Peer-to-Peer Electronic Cash System
"A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution."
– Satoshi Nakamoto
SO, "PEER-TO-PEER" WOULD BE LIKE YOU GIVING ME FIVE BUCKS FOR THESE COOKIES, RIGHT?
YES AND NO.
NEARLY ALL FORMS OF TRADITIONAL PAYMENT HAVE LAYERS OF INTERMEDIARIES, INCLUDING "FIAT" CURRENCY SUCH AS THIS.
SO, WHY IS THAT A PROBLEM?
AND DON'T GIVE ME THE WHOLE HISTORY OF MONEY.
GOOD QUESTION, LITTLE GIRL.
BUT FIRST, LET'S LEARN ABOUT THE HISTORY OF MONEY...
UGH
In early agrarian societies, those with ... such as livesto... ed:
Alas, I hav... five goats, b... grain to fee...
STOP!
STOP!
I KNOW THIS ALREADY: STONES OR TRINKETS LEAD TO PRECIOUS METALS LEAD TO COINS LEAD TO PAPER NOTES LEAD TO MODERN BANKING OR PAYPAL OR WHATEVER—
—BUT WHY DO WE NEED A NEW WAY?
!
WELL, HOW ABOUT BECAUSE, UNDER TODAY'S FINANCIAL INFRASTRUCTURE, MONEY IS:
1 PRONE TO INFLATION AND MISMANAGEMENT.
2 INCREASINGLY NOT PRIVATE.
3 TOO EASY TO HACK.
4 SPLINTERED INTO 180 SLOW-TO-TRANSFER LOCAL CURRENCIES.
5 HARD TO DIVIDE INTO SMALL INCREMENTS.
6 PLAGUED BY GROWING TRANSACTION FEES.
7 AND LARGELY INACCESSIBLE TO ABOUT TWO BILLION PEOPLE.

OKAY OKAY.
OUR MONEY SUCKS.
BUT HOW CAN I TRUST THAT "PEER-TO-PEER ELECTRONIC CASH" WON'T BE EVEN MORE FLAKY AND UNSTABLE THAN WHAT WE HAVE NOW??
SO, THE KEY IS—
—DON'T RELY ON "TRUST!"
AH! WHO THE HELL ARE YOU?
I AM SATOSHI NAKAMOTO.
WAIT—I THOUGHT THAT GUY WAS SATOSHI NAKAMOTO!
WRRRRRR...
TELL ME SOMETHING: SUPPOSE I GAVE YOU THIS GOLD BAR FOR YOUR COOKIES...
!!
O-KAYY...
SO, NOW I CAN EAT THE COOKIES, BUT I'LL BET YOU CAN'T EAT THE GOLD, RIGHT?
OOF!
NO, BUT I COULD SELL IT AND BUY 100,000 MORE BOXES!
EXACTLY. GOLD IS RARE—
—PLUS DESIRED AND THUS VALUED—
—AND THAT VALUE IS VERIFIABLE—
—AND NON-REPRODUCIBLE.
BUT NOW, LET'S SUPPOSE WE GIVE GOLD TWO ADDITIONAL PROPERTIES:
EXTREMELY PORTABLE—
WH— HEY!
—AND DIVISIBLE—
K-PASH!!
ACK!
—DOWN TO INFINITESIMAL FRACTIONS IF NEEDED!

HERE'S YOUR **FIVE DOLLARS**, BY THE WAY.
STUPID TEMPORARY METAPHORS...
NOW IF ONLY WE COULD **SEND THAT STUFF** TO ANYONE ELSE ON EARTH WITH THE **PUSH OF A BUTTON...**
VOILA!
WE'D HAVE **TRUE WORLDWIDE PEER-TO-PEER CASH!**
YEAH, YEAH... NICE **FANTASY.**
BUT I KNOW WHERE THIS IS GOING, PAL, AND **NUMBERS** OFFER THE **EXACT OPPOSITE** OF WHAT GOLD OFFERS!
TRUE.
GOLD
✓ RARE
✓ VALUED
✓ VERIFIABLE
✓ NON-REPRODUCIBLE
# NUMBERS
→ COMMON
→ VALUELESS
→ FAKEABLE
→ HELLA REPRODUCIBLE
→ ALSO BORING
YET, IN THE **REAL WORLD,** IF YOU **DID** OWN GOLD, **"NUMBERS"** MIGHT BE ALL YOU EVER SEE.
TELL ME, WHAT'S YOUR **NAME?**
ALICE.
HA! HA! **PERFECT.**
??
SO, IF **"ALICE"** OWNS **$5.00** IN GOLD—OR **ANY** ASSET OF VALUE—THE REAL STUFF MIGHT BE HALF A WORLD AWAY, RIGHT?
SURE.
ALICE REALLY JUST HAS HER NAME ON A **LEDGER** SOMEWHERE, STATING HER OWNERSHIP.

owner	share
Alice	$5.00

IF ALICE GIVES **$2.00** TO, SAY, **"BOB,"** THE ASSET NEVER MOVES. ONLY THE **LEDGER** CHANGES.
GOT IT.

owner	share
Alice	$3.00
Bob	$2.00

ALSO, BOB'S COOL.
BEHIND A WALL OF SECRECY, A **"TRUSTED THIRD PARTY"** SUCH AS A **BANK** OR PUBLIC INSTITUTION MAINTAINS THE LEDGERS.
IT'S ALL HERE.
AND WE **HOPE** OUR TRUST WILL NEVER BE **BETRAYED** THROUGHOUT THE LIFETIME OF OUR ASSETS.
UH OH.
WE ALSO ENTRUST SUCH THIRD PARTIES WITH A TON OF OUR **PRIVATE INFORMATION—**
Hi Bob!
Hi, Alice
—EVEN THOUGH WE'RE NOT ALLOWED TO PENETRATE **THEIR OWN** WALLS OF **SECRECY.**
Hey!

d790ed6	d986116	a855b0f	90e9481	16236c9	c00d1cf
0.00	0.00	768.31	996.24	346.60	4845.87
5.00	0.00	201.46	1246.18	341.12	7014.12
3.00	2.00	2705.33	1446.18	796.10	124.75
2.00	3.00	3308.55	301.42	4556.76	9739.85

TRUE PEER-TO-PEER CASH DOESN'T NEED "TRUST." JUST ONE GIANT LEDGER THAT EVERYONE CAN SEE—
—WITH EACH ENTRY TIED ONLY TO A USER'S CRYPTOGRAPHIC KEY—SO NOW THE USER IS THE ONE BEHIND A WALL OF PRIVACY.
ANY QUESTIONS SO FAR?
OMIGOD— SO MANY QUESTIONS....
LIKE WHO MAINTAINS THE LEDGER, HOW DO THE KEYS WORK, WHY IS ANY OF IT WORTH ANYTHING—
—AND WHAT IN THE WORLD IS A "COIN" IN THE FIRST PLACE??
WE DEFINE AN ELECTRONIC COIN AS A CHAIN OF DIGITAL SIGNATURES.
ACK!
SATOSHI, WHAT IS THIS TH—
OH NO.
I AM SATOSHI NAKAMOTO.
GULP!
UH...
OKAY THEN... S-SATOSHI... "CHAIN OF DIGITAL SIGNATURES," WAS IT?
CORRECT!
_HUMAN-NAME-OF: ALICE TRANSFERS .001 BITCOIN TO _HUMAN-NAME-OF: BOB BY DIGITALLY SIGNING HASH OF PREVIOUS TRANSACTION AND PUBLIC KEY BELONGING TO _HUMAN-NAME-OF: BOB AND APPENDING TO END OF COIN.
IT IS EASILY SHOWN:
Transaction
Owner 1's Public Key
Hash
Owner 0's Signature
Transaction
Owner 2's Public Key
Hash
Owner 1's Signature
Owner 2's Private Key
Transaction
Owner 2's Public Key
Hash
Owner 2's Signature
Owner 3's Private Key
Verify
Sign
Verify
Sign
WHOA WHOA— SLOW DOWN!
DOES MY FORM NOT PLEASE HUMAN-NAME-OF: ALICE ?
NO NO NO DON'T CRY! IT'S NOT THAT! I JUST...
I BRING EXPLAINING GIFT.
A RUBIK'S CUBE? HEY, WAIT A MINUTE... THEY USED THIS ANALOGY IN MATH CAMP...
"EASY TO SCRAMBLE, HARD TO UNSCRAMBLE." RIGHT!
I REMEMBER HOW THE KEYS WORK NOW, THANKS!
ANYONE CAN SEND STUFF TO ME USING MY PUBLIC KEY TO ENCRYPT IT, BUT ONLY MY PRIVATE KEY CAN DECRYPT IT.
PRIVATE
PUBLIC

AND THE "HASH"... THAT'S A SCRAMBLED VERSION OF THE LAST TRANSFER?
CORRECT!
Public Key
Hash
Owner 1's Signature
Ver
SO, YOU'RE NOT JUST VERIFYING NEW COIN OWNERS; YOU'RE CREATING A CHAIN OF OWNER-KEYS ALL THE WAY BACK TO A COIN'S BIRTH—A HARD-TO-BREAK CHAIN!
HARD LIKE MOUNTAIN OF CUBES!
HEY, IS THIS THAT "BLOCKCHAIN" EVERYONE'S BEEN GOING ON ABOUT?
NOT QUITE.
THE BLOCKCHAIN IS A NEW KIND OF LEDGER. WE'LL GET BACK TO THAT—
—BUT YEAH, THAT HISTORY OF OWNER KEYS IS PART OF IT.
UH...
YAY! I AM BEST HELPER!
LEMME GUESS...
SATOSHI NAKAMOTO AT YOUR SERVICE.
SO, THAT CHAIN OF OWNER-KEYS ISN'T A STRAIGHT LINE; COINS SPLIT AND MERGE A LOT, SO IT LOOKS MORE LIKE A FAMILY TREE.
ASSUMING YOUR FAMILY'S INTO ASEXUAL REPRODUCTION AND FUSION, SURE...
SO, LET'S SAY ALICE HAS ONE COIN THAT'S WORTH $5 AND WANTS TO GIVE BOB $2 WORTH...
HER $5 SERVES AS THAT TRANSACTION'S 'INPUT'; IT'S THE AMOUNT ENTERING INTO THE TRANSACTION.
5
BUT, THERE ARE TWO 'OUTPUTS': THE $2 ALICE GIVES BOB, AND THE $3 IN CHANGE SHE GIVES HERSELF.
OUTPUTS
WEIRD.
2
3
"WEIRD," YES, BUT EFFICIENT. BOB GIVING CHANGE OR YOU SPLITTING IT BEFOREHAND WOULD'VE MEANT SEPARATE TRANSACTIONS.
HUNH.
NOW IF BOB TAKES THAT $2 AND ADDS TWO $1 COINS, HE CAN USE THOSE MULTIPLE INPUTS—
1
1
2
—TO CREATE A SINGLE OUTPUT OF $4 THAT HE GIVES TO CAROL.
OUTPUT
HEY!
SHE PAID FOR PIZZA!
4

A BALANCE-BASED SYSTEM MAY SEEM SIMPLER (AND MOBILE WALLETS CAN ALWAYS OFFER THAT EXPERIENCE)—
ALICE
BOB
CAROL
—BUT BALANCES TEND TO BE TIED TO THE IDENTITIES OF ACCOUNT-HOLDERS.
HEY, THAT'S MY GLA-
OH. HAHA
WHEREAS THIS WAY, OWNER-KEYS MAY COME AND GO...
AHH... BUT IT'S THE COIN'S IDENTITY THAT LASTS!
EVERY COIN IS ACCOUNTED FOR. ABOUT 17 MILLION FULL BITCOINS HAVE ENTERED THE SYSTEM, AND BY 2140 ALL 21 MILLION WILL BE OUT THERE.
THE SUM TOTAL OF THE LATEST ENDPOINTS ON EACH AND EVERY FAMILY TREE IS THE UTXO OR 'UNSPENT TRANSACTION OUTPUT'—
—THE BITCOIN EQUIVALENT OF ALL THE MONEY IN THE WORLD.
COINS MERGE AND SPLIT; THEY SKIP FROM KEY TO KEY, BUT THEY NEVER REALLY GO ANYWHERE.
THEY WERE NEVER 'ANYWHERE' TO BEGIN WITH.
WHAT HAPPENS IF I LOSE MY KEY?
NOTHING. THOSE COINS JUST STAY UNCLAIMED. MAYBE FOREVER.
THIS IS WHY, IN THE LONG RUN, THE CURRENCY IS GENTLY DEFLATIONARY. THE CIRCULATING COUNT WILL GRADUALLY DWINDLE...
AFTER 2140.
YUP.
BUT IT'S STILL JUST NUMBERS! WHY CAN'T ME AND FIVE FRIENDS IN FIVE COUNTRIES BUY FIVE CANDY BARS USING THE EXACT SAME KEY AND COINS? ...THEORETICALLY...
THE ONLY WAY TO CONFIRM THE ABSENCE OF A TRANSACTION IS TO BE AWARE OF ALL TRANSACTIONS.
!
GOOD POINT, SATOSHI—WHO'S NOW A MONKEY, I GUESS...
THAT'S WHY WE NEED A UNIVERSAL PUBLIC LEDGER ISN'T IT?
YES.
INCLUDING A TIMESTAMP SERVER.
YOUR CRIMINALLY-INCLINED FRIENDS ARE POSING WHAT WE CALL A "DOUBLE-SPEND" PROBLEM.
"CRIM—" HEY!
THEY'RE NOT—
I MEAN—

...
OKAY, I... DON'T REALLY HAVE FIVE FRIENDS...
FINE THEN: FIVE FRIENDS—NONE OF WHOM KNOW OR LIKE YOU—WISH TO SIMULTANEOUSLY SPEND IDENTICAL COINS AND KEYS IN EXCHANGE FOR FIVE CANDY BARS.
CANDY
CANDY
CANDY
CANDY
CANDY
A PEER-TO-PEER DISTRIBUTED TIMESTAMP SERVER WOULD GENERATE PUBLIC PROOF OF THE CHRONOLOGICAL ORDER OF TRANSACTIONS, AND DEEM ONLY THE FIRST CONFIRMED AS WORTHY.
✓
BETTER STILL, IF PENDING TRANSACTIONS ARE BROADCAST QUICKLY TO ALL NODES, ONLY ONE WOULD EVEN BE SEEN BY A GIVEN MERCHANT. POOR ODDS FOR THE WOULD-BE SCAMMER.
?
BUT IN THE END, DOESN'T ONE RANDOM GUY ACTUALLY GET THE CANDY BAR?
YES. THE SYSTEM HAS BEHAVED AS DESIGNED.
ONE SUCCEEDS. IT MATTERS NOT WHICH.
LUCKY GUY!
HE WILL SUFFER TOOTH DECAY AND DIE UNMOURNED, A DISGRACE TO HIS FAMILY.
WHATEVER... SO, I GET WHY WE NEED DISTRIBUTED TIMESTAMPING FOR CONFIRMATION.
BUT WHY DO SO MANY PARTICIPATE IN IT?
AYE, LASS. "WHY," INDEED! WHY DO WE TOIL NIGHT AND DAY?? WHAT FIRE, DEEP IN OUR CAVERNOUS BELLIES, RISES TO POWER THE MIGHTY FORGE OF OUR SOULS—TO COMPEL OUR ARMS TO DIG AND HOIST AND—
IT'S FOR THE MONEY ISN'T IT?
AYE, IT'S THE MONEY. HELPING TO CONFIRM TRANSACTIONS MIGHT WIN YOU SOME BITCOIN...
ALSO TRANSACTION FEES!
HEY, AREN'T YOU GUYS GERMAN?
WE ARE SATOSHI NAKAMOTO!!
NO, NO, I MEAN—
—DON'T DWARVES COME FROM GERMAN FOLKLORE? I THOUGHT THERE WAS SOME KINDA JAPANESE THEME GOING ON HERE...
NO ONE TOLD US THERE WAS A THEME.
I TOOK HOURS PUTTING THESE ON...
NEVER MIND. SO WHEN I GIVE BOB BITCOIN, THAT STARTS AS A PENDING TRANSACTION. DO YOU SEE THAT RIGHT AWAY?
AYE! AND MANY MORE LIKE IT!

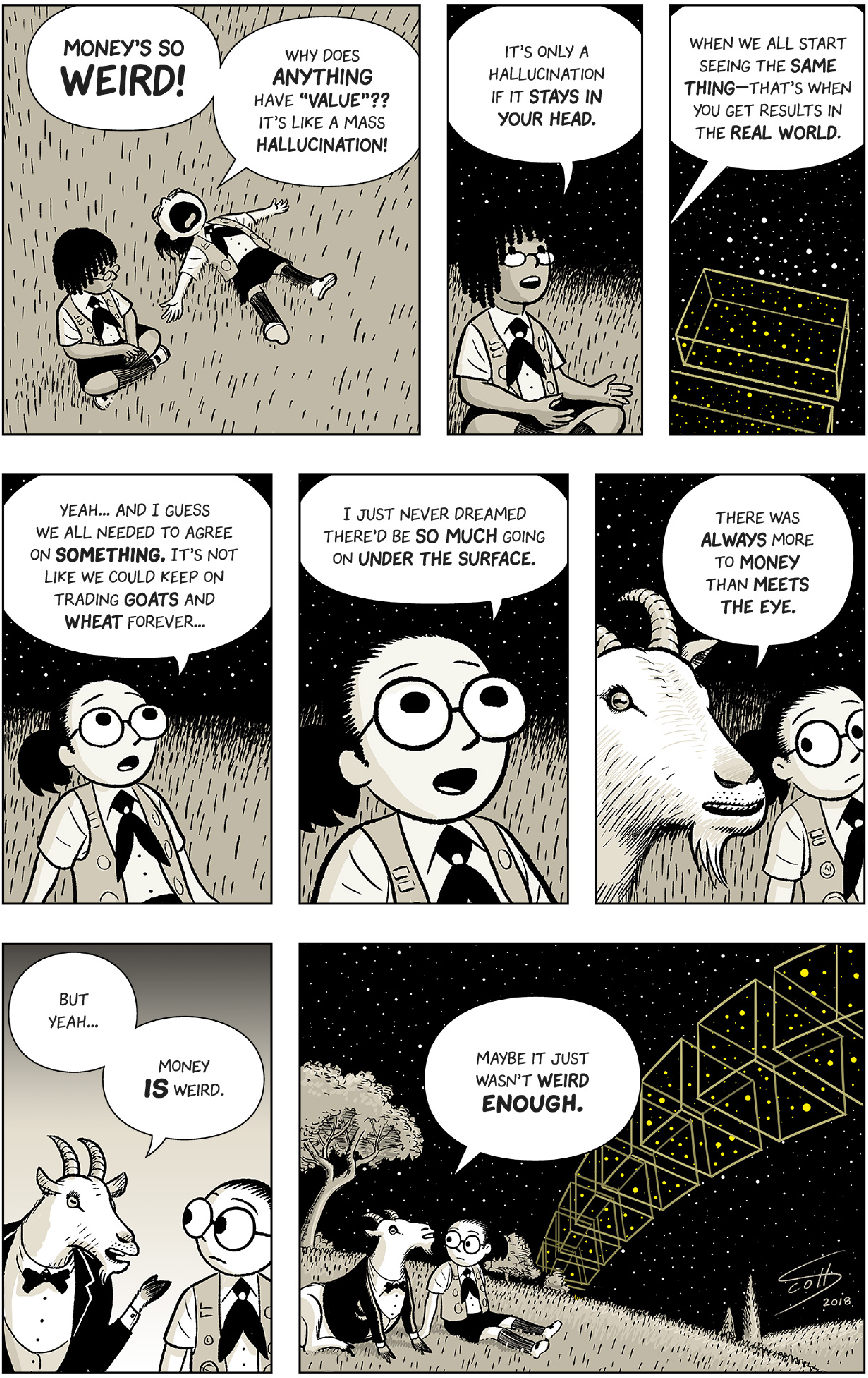
```
Input:
Previous tx:
c14ca9164792c453362a57f99235d58168908c5f85060030ddb2d4a00cfd2dd4
Index: 0
scriptSig:
26e6631530817fe35c2a42064b085e61934d8368bcc8c28385bf9fd2798f0f073d00
9e782c14ca9164792c453362a57f99235d58168908c5f85060030ddb2d4a00cfd2dd
4bb4cf5a

Output:
Value: 5000000000
scriptPubKey: OP_DUP OP_HASH160
65b6be5ecb63294560df81492125483020634ea8
OP_EQUALVERIFY OP_CHECKSIG
```

BEHOLD! ONE COMES NOW!
OMIGOD, THERE THEY ARE! THE INPUT AND OUTPUT FIELDS, THE KEYS...
EVEN THE HASH OF THE PREVIOUS TRANSACTION!
HEE-HEE! IT'S LIKE WE'RE SPYING! THIS IS REALLY HAPPENING SOMEWHERE!
AYE, THOUGH WHERE OR TO WHOM WE CAN ONLY GUESS!
HANG ON—DOES THAT SAY "VALUE: FIVE BILLION"??
AYE! BUT 'TIS ONLY FIVE BILLION 'SATOSHIS'—OUR TINIEST DENOMINATION AT ONE HUNDRED MILLIONTH OF A BITCOIN.
SO THAT'S A FIFTY!
ALL DAY AND NIGHT THEY DESCEND: A MERCILESS, NEVER-ENDING HAILSTORM OF NEW TRANSACTIONS!
BUT NO SOONER DO THEY HIT THAN WE SHOVEL THEM INTO A MIGHTY BLOCK—
—AND COMMENCE TO MINING!
KINDA ABANDONED THAT METAPHOR JUST NOW, DIDN'T WE?
AYE, IT WAS UNSUSTAINABLE...
BUT HEY—DID I HEAR THE WORD "BLOCK"?
INDEED, LASS! THE BLOCKCHAIN IS UPON US!
SO, IF EACH MINER FILLS THEIR OWN BLOCK, WON'T EACH BLOCK HAVE DIFFERENT TRANSACTIONS?
ONLY SLIGHTLY SO! MOST GRAB 'EM IN THE ORDER THEY HIT THE NETWORK.
IF YOUR TRANSACTION WITH THAT RASCAL BOB DOESN'T MAKE THE WINNING BLOCK, IT'S SURE TO BE IN THE NEXT ONE.
OOH! WHAT MAKES A "WINNING BLOCK"? CAN I WIN?
YOU CAN... IF YOU SOLVE A DEVILISHLY HARD PUZZLE REQUIRING TRILLIONS OF CRYPTOGRAPHIC GUESSES.
OH.
WELL, THAT SOUNDS LIKE A LOT OF WORK.
EXACTLY.

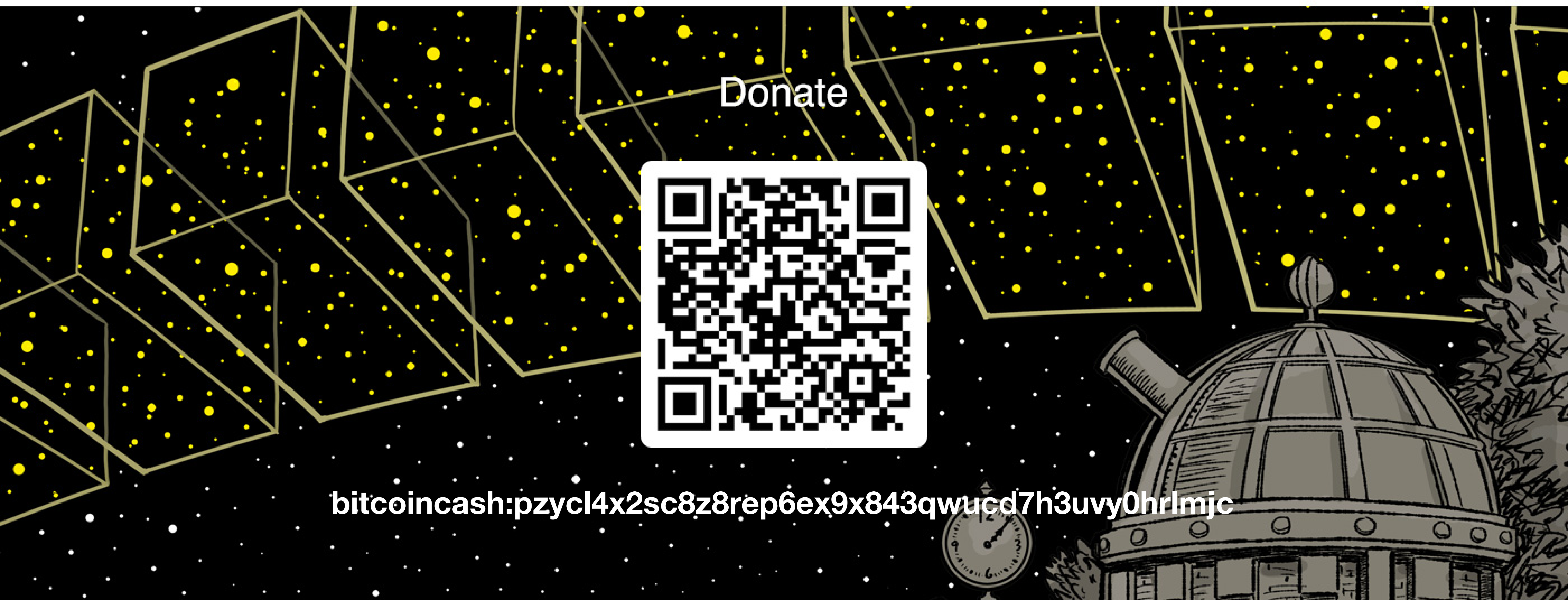
WORK IS THE FIRE THAT FORGES THE CHAIN!
WORK IS THE ORIGINAL CURRENCY!
RRAAAR!
WOO! HOO!
YYEAH, I HAVE NO IDEA WHAT THAT MEANS...
WELL, TO START, EACH BLOCK HAS CERTAIN INGREDIENTS.
INCLUDING THE MANY TRANSACTIONS BEING VALIDATED—
NAKAMOTO
—THEN A SEPARATE HEADER CONSISTING OF THE PREVIOUS WINNING BLOCK HASH—
—THE "MERKLE ROOT"; A HASH OF THE HASHES OF EVERY TRANSACTION—
—ASSORTED META-DATA—
—A ONE-TIME RANDOM NUMBER CALLED A "NONCE," AND FINALLY, THE TIMESTAMP—
*
TICK TICK TICK TICK
*NOT SALT
—ADDED JUST AS WE SCRAMBLE IT ALL WITH THE POWERFUL SHA-256 HASHING ALGORITHM, ANND...
WHRRRR!
NOPE. NOT RIGHT.
WHAT ARE YOU LOOKING FOR?
METAPHORICALLY, A PERFECT OMELETTE—BUT OKAY, LITERALLY: A 64-DIGIT STRING LOW ENOUGH TO START WITH AT LEAST 17 ZEROES...
e51cd7f548 780f1e1c7bbf0b 0da1156dd71dcd0e 56ead64218ca2c 67a62957da
BUT THAT'S IMPOSSIBLE!
NO, JUST VERY, VERY UNLIKELY.
AND SO, ANOTHER TRY—
—BUT NOW WITH A NEW TIMESTAMP, A NEW RANDOM NUMBER, AND MAYBE A BETTER RESULT!
PFT CAN'T UNSCRAMBLE AN EGG, BUDDY.
NO PROBLEM. SPECIALIZED MINING UNITS CAN HASH A TRILLION JUST LIKE IT EVERY SECOND FOR AS LONG AS IT TAKES!
!!

NOW YOU SEE WHY THEY CALL IT "PROOF OF WORK."
WH—ZELDA?! WHAT'RE YOU DOING HERE?
I'M SORRY, I DON'T THINK WE'VE MET. I'M SATOSHI NAKAMOTO.
OH... RIGHT.
OF COURSE.
SO YOU SEE, IT TAKES THE HARD "WORK" OF MANY PROCESSORS TO CLEAR THAT CRYPTOGRAPHIC THRESHOLD.
00000 000000000 0000e8fd1 0a42cf715 829f493fb a37931ea2 32f479fe0 76ce6
BY DESIGN, ONE NODE (AKA "MINER") HITS THE JACKPOT ABOUT EVERY TEN MINUTES. IF THINGS SPEED UP OR SLOW DOWN, THE DIFFICULTY ADJUSTS ACCORDINGLY.
THE LUCKY NODE RECEIVES NEWLY-MINTED COINS (12.5 CURRENTLY—HALVED EVERY FEW YEARS) AND THE OTHER MINERS VERIFY THE RESULTS FOR THEMSELVES.
IF THE MATH CHECKS OUT, THEY START WORKING ON THE NEXT BLOCK AS AN EXTENSION OF THAT NEWLY-CONFIRMED BLOCK.
NODES "VOTE" BY CONTRIBUTING COMPUTATIONAL POWER.
THEY COULD BUILD ON ANY CHAIN, BUT IT'S IN THEIR ECONOMIC SELF-INTEREST TO BUILD ON THE SAME CHAIN AS EVERYBODY ELSE.
WHY IS THAT?
BECAUSE THOSE NEWLY-MINED COINS (THE NODE'S REWARD) CAN ONLY HAVE VALUE—
—IF THEY'RE ACKNOWLEDGED AS VALID BY THAT CONSENSUS CHAIN.
OTHERWISE...
POOF
THE MARKETPLACE WON'T EVEN SEE THEM.
EVEN IF A GREEDY ATTACKER COULD ASSEMBLE MORE CPU POWER THAN ANYONE ELSE, HE'D BE BETTER OFF MINING NEW BITCOIN THAN DEFRAUDING THE SYSTEM THAT GIVES THEM VALUE.
SELF-INTEREST, INSTEAD OF TRUST, HOLDS THE SYSTEM TOGETHER.
STILL WANNA PUT YOUR TRUST IN SOMETHING?
TRUST THE MATH.

A BIT GRANDIOSE, DON'T YOU THINK?
SORRY. THE SKY IS LITERALLY THE ONLY THING EVERYONE ON EARTH CAN SEE...
NOTICE THOSE BIG STARS, APPEARING ONE BY ONE NEXT TO THE LATEST BLOCK? THEY'RE NEWLY-RECEIVED TRANSACTIONS, ACCUMULATING WHILE NODES WORK ON FINDING THE NEXT BLOCK'S WINNING NUMBER.
WAIT FOR IT...
AND... CONFIRMED!
A NEW BLOCK HAS JOINED THE CHAIN.
WITHIN THOSE BLOCKS, YOU'LL FIND ALL THE FAMILY TREES OF PAST KEY OWNERS.
ALL THE MERGED AND SPLIT COINS DESCENDED FROM EACH BITCOIN'S BIRTH AS A BLOCK REWARD—
—WHETHER FROM 9 YEARS AGO OR LAST WEDNESDAY.
END RESULT: A PERSISTENT, TRANSPARENT, PEER-TO-PEER, APPEND-ONLY LEDGER OF TRANSACTIONS THAT ANYONE CAN ADD TO BUT NO ONE CAN CHANGE.
MESS WITH ONE PENNY OF VALUE OR ONE SECOND ON A DATE AND ALL THOSE HASHES FREAK OUT LIKE SOME CRYPTOGRAPHIC "BUTTERFLY EFFECT."
BUT... IF IT'S ALL SO SECURE, WHAT WAS THAT WHOLE "MOUNT GOX" THING ABOUT?
"MTGOX" WAS AN EXCHANGE— MORE LIKE A BANK REALLY. PEOPLE TRANSFERRED BITCOIN TO MTGOX ADDRESSES FOR SAFEKEEPING, WHICH TURNED OUT TO BE A MISTAKE.
OUCH
NO ONE HACKED THE MONEY. THE MONEY WORKED FINE. THAT'S WHY IT WAS WORTH STEALING IN THE FIRST PLACE.
IS IT TRUE THAT PROOF OF WORK USES A LOT OF POWER?
YEAH.
THAT'S COME UP A LOT LATELY...
BUT IT'S IMPORTANT TO WEIGH THE COSTS OF A SYSTEM WITH THE UTILITY AND VALUE IT PROVIDES. PEER-TO-PEER ELECTRONIC CASH COULD OFFER WORLD-WIDE BENEFITS AFTER ALL.
"UTILITY"... "VALUE"... UGH


MONEY'S SO WEIRD!
WHY DOES ANYTHING HAVE "VALUE"?? IT'S LIKE A MASS HALLUCINATION!
IT'S ONLY A HALLUCINATION IF IT STAYS IN YOUR HEAD.
WHEN WE ALL START SEEING THE SAME THING—THAT'S WHEN YOU GET RESULTS IN THE REAL WORLD.
YEAH... AND I GUESS WE ALL NEEDED TO AGREE ON SOMETHING. IT'S NOT LIKE WE COULD KEEP ON TRADING GOATS AND WHEAT FOREVER...
I JUST NEVER DREAMED THERE'D BE SO MUCH GOING ON UNDER THE SURFACE.
THERE WAS ALWAYS MORE TO MONEY THAN MEETS THE EYE.
BUT YEAH...
MONEY IS WEIRD.
MAYBE IT JUST WASN'T WEIRD ENOUGH.
Scott 2018

CoinSpice



Donate

bitcoincash:pzycl4x2sc8z8rep6ex9x843qwucd7h3uvy0hrlmjc