

Aug 2007.

Bitcoin

~~Electronic Cash~~ without a payment intermediary

An essentially Peer 2 Peer electronic cash system could allow online payments to be exchanged directly from one party to another without the hassle of exchange using a financial intermediary. Digital Signatures offer a part of the solution, but the primary benefits are lost if an intermediary based on trust is required to ensure that a transaction can not be double spent.

We propose a solution to the double spending attack vector based on the universal broadcast of transactions over a tightly connected p2p network. The network of commercial nodes competes to form a time stamped record of transactions that are ~~are~~ ordered chronologically.

Competitive systems act as nodes that record transactions in a sequence or chain of hash based effort proving the economic cost spent in creating the work. A set of records in a manner that precludes altering one value without returning to calculate all proof values in the sequence. The longest chain of hashes serves as both a chronological sequence of ordered events and a public record of all events. It acts as a witness to the received order of events and is a set of proof and acts as an evidence trail showing that the majority of the systems acting to validate transactions hold the largest economic investment and

expenditure via the most "wasted" CPU power.

Whilst honest nodes are operated and controlled by the largest amount of CPU burning over the connected network of validator companies, these competing systems generate the longest chain and outpace an attacker.

A highly connected small world form network that broadcasts to all connected nodes (see notes on NIPAA @ ASX) only need a basic structure and self forms and is self healing and resilient to attack and/or outage.

Transactions are sent to all nodes using a "broadcasted basis by best effort.

Groups and Systems competing to act as a validator and to earn revenue are not required to be a part of the ongoing system and can leave and/or rejoin the system at will picking up where the last value was validated. The nodes use the longest valid chain of work evidenced hash expenditure in order to validate as a commonly accepted ledger of occurrences that can be validated even though some nodes come & go.

## Intro.

Commerce on the Internet has ~~come~~ become almost totally reliant on the use of risky, costly, financial payment intermediaries.

Micro payments and small online token payments have been promised for decades (Tim Mar - Blacknet → Speler)

The trust needed is too high  
transaction costs are too great.

Disputes cannot be arbitrated without costs that preclude small casual payments & any web pay by page system.

Fraud cannot be avoided (see Branger re Fraud Triangle and idea

of triple entry ledger)

Merchants hold PII

- adds to cost & risk.

Non-reversible - small games - Wow

Web has no physical currency tokens.

like a coin as noting can be done  
for under 1¢.

An electronic payment system that is  
based on costly to cheat evidence is

required - (e-cash failure as Double  
spends and IAA are too costly but

anonymous. = tolls and rewards.

This shield of rewards always leads  
to the worst factor in society collapsing  
the system (Plato - Ring of Gyges).

Q → why do ppl think privacy and  
anonymity are even close ...

Anonymity is the tool of criminals and the dark state actor.

Privacy is honest.

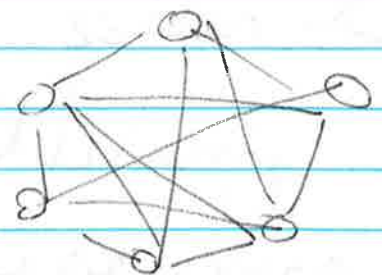
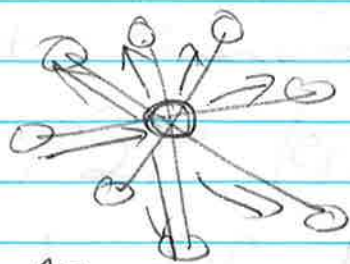
If a system is anonymous it cannot be private — ever!

Privacy is to Anon

as Good is to utter Evil!

Always Double spends - how to have a system with no intermediary

Answer - the ASX (NIPPA) was a central & hub spoke



If we take the centre and have this removed as a complete broadcast

like many P2P pirates are using to avoid honest payments, we can use the tools the criminals advanced against them.

P2P File theft networks do not care about double-spends - the information is "free" or has no value (socialist) we just need to have ~~an~~ a time ordered economically enforced ledger of all transaction messages that all parties can validate.

The ledger + economics solves the crime of P2P (criminal) sharing networks and defeats these parasites. We create a distributed commercial P2P timestamping service where



parties compete to validate a separate  
IP 2 IP per exchange network  
exchange ordering these in a FIFO  
structure.

if we take the use of code as a  
predicate we can build a TTM or  
as Sipser called it, a decider.

$T$  is Valid = True

is False = Reject.  
as not Valid

The system is economically secure.  
The chain of  $T$ 's mean that a  
Red queen game eventuates where  
an attacker is always behind the  
honest group.

⇒ unlikely that a criminal  
majority could eventuate.

for the criminal groups to gain a majority they will need to run more systems  $\rightarrow$  sustainably than the honest ones.

$\rightarrow$  We would expect the creation of Data Centres & large server farms. If the timechain concept works. A data centre is easy to find and as it takes a capital investment over time is difficult to Sybil.

Thus - we can expect that criminals and other dishonest groups who have resulted in the collapse of all other digital cash systems, will not be attracted to my system.

(Lynn's Law tutor may be at

use here and has a contact to the  
KPMG legal guy in Melb who uses  
an e-cash tracing paper).

## Transactional Message

A digital coin is formed using a  
chain of digital signatures.

The User transfers the coin to the  
user they want to exchange with.  
(see Northumbria notes)

— If User to User, we can  
say this is a direct exchange

— But → as a backup we send  
to the network & they hold a  
transaction for a defined time (\*?)  
to be sent to the recipient when they  
check the network.

(Ozemail - VUCP analogy).

(Northumbria - if this is not User 2 User, it would be likely a Postal Rule exchange in UK law)

In the past systems, users cannot directly verify that a transaction was not been double spent already. This is why an intermediary exists - to report + stop double spends

What if:

It is a self-help network that is all users can see the chain of validator messages and can check if the coin they are offered has been presented previously themselves?

The ecash (90's) process needs a

mint & acts as a depository bank but this is not efficient

→ again cannot do small payments & kills web commerce.  
If we have an ~~not~~ overlay structure where all transactions are public, this means that any user can instantly validate the state of the transaction that they are to receive.

An intermediary has always been necessary.

Aiming to all parties means all can check — but not all need hold all

The time chain is crucial as all parties must agree on the order of a transaction and a single history

results. (No more Euro & many books - Watty!)

the user receiving a payment thus needs evidence detailing the true time of every transaction as the majority of validating companies have agreed to state (in open competition) is the true history of what was 1st received - FIFO model.

(Tracing law seems to be heavily on FIFO. - see case).

Also Mobox & Smart card tracing orders.

Time stamp and ordering Server.

We start with a distributed time and validator (or order reporting)

server.

The server is a distributed group of peer systems - commercial entities act to compete.

Each seeks payment by transaction fees earned in validating a batched set of transactions.

(see Brooks as well).

We ~~to~~ batch a set of messages into a single block and then hash this (order now matters)

The hash of this block of batched transactions and/or messages - This is similar to what

S. Haber / WS Starnetta (1991)

(1997)

proposed using newspapers and

UseNet. We use this public source of hash (one way) information in order to timestamp a batch of digital messages.

If we ~~not~~ link the hashes (see the Lamport chain) so that a hash also has the hash in the batch from the last batch - we end with a chain.

Like Lamport (Lesley) and his signature scheme, the chain is now more secure as it extends.

## Network

The network consists of a P2P user layer on top of a P2P (commercial) validation layer. This will



solve if the system works.

1) All new messages are received by nodes on the network and are then broadcast to all other active nodes.

2) Each node in the commercial validator network orders the messages into a batch.

3) Each node seeks to solve a difficult puzzle.

Aura et al have an interesting idea on a hash ~~base~~ based puzzle where you seek to find a partial hash collision.

See more Aura.

This puzzle can be <sup>to use</sup> matched against the

hash of the block formed at the last value hash and the batch of time (strictly) ordered (chronologically) transaction messages.

4) When a validator in the Peer group finds a solution to the hash puzzle (see also mod square options) it seeks to broadcast this to all other validators as fast as it can.

→ Note these commercial entities compete for the batch fees (the guys QSCU use & D have can act as a model → even if single entity & Bank).

5) The nodes validate the batched block, its contents, and the solution to

The puzzle seeking (a zero sum game  $\rightarrow$  set reward per period) to invalidate the competing nodes in any error (as this increases the overall revenue of each node with a goal + honest approach).

— batches must only have valid ~~for~~ transactions that are not double spent.

b) After validating the batch - the reward is paid to the winning node and the nodes in the group accept this - demonstrate acceptance) is then using the discovered puzzle value to move onto building the next batch.

The hash of the accepted block is included in the next batch & block.

→ Note - Nodes will work on the longest chain (should keep other - in case) seek to extend the longest chain.

If two (or more) forks exist, then as the world is large and this is distributed, we end with a race and fork of the chain - this ends through competition.

Users - Do not care Users have SPV

This is a validator issue (need to have validator rewards unspendable for a significant time to make certain that forks do not lead to invalid spends - the only

issue - maybe have validators need a day's grace before being able to spend revenue?

See Small world - we would expect the validators to be densely connected.

This means - we can expect any transaction volume  $\rightarrow$  Terra bytes at a time to be sent  $\rightarrow$  commercial entities seek profit and the network will scale as these companies invest to capture profit.

Faster sanding of the batch & the solution = more revenue.

The system goes to an equilibrium where the revenue and cost balances

far, where the cost of scaling leads to a system that costs more than the fees to maintain.

— P2P & Fault-tolerant

— Dropped Transactions etc are OK.

— Inefficient nodes (companies) are going to earn less and be dropped.

~~if the~~

incentives — This is an economic model & companies compete.

We will jump start with a subsidy

→ see Singapore / Korea.

→ reward miners & validators.

→ like seeking Gold.

→ As more - value per subsidy decreases to mean the validator effort

the uneconomic payment but to allow them to see that they need to compute and hence professionalise and this means to grow the transaction volume AS LARGE AS Can be by any legal method

There is 10% limit to scaling

The P2P FEED cash system uses

any message + time stamp will add fees and make the cost of fees to

the micro payment use less

→ More transactions

→ Larger Batches

→ Stronger more professional network.

Companies Build & Create a complete system.

Explain + detail Fees.

TBD.

Note it is the incentives that allow the system to professionalise as the message value grows.

→ Moore Law.

There is no limit to scaling

The P2P digital cash system once it has been bootstrapped.

(even pay for Page

- No more Ad's)

Dishonest validators end

→ In Law!

→ In being rejected by honest nodes seeking to grow the network.



## Size + Space

Storage Doubles faster than Moore's Law.

But we can prune old values when the chain is deep enough.

→ likely way back chain is an archive.

## Percept Memory vs Storage.

### User Payment Network

The user acts on a simplified network - only need batch of message headers.

Alice (A) wants to send to Bob (B)

A → B.

A sends the path & hashes.

(i.e., A proves here message & the fact

the coin she has received has not

been spent.

Merkle vs other trees.

→ to check more.

Attack only ends as a double spend  
and this is like cheque fraud with  
signed evidence (law).

Perceptron

Fan in / Fan out.

need to cover the Minsky stuff.

One / Many Inputs



One / Many Outputs.

(change as a concept)

lots of coins

— like minting +

re minting

but all users do this themselves

Simple Payment is for Users

Users Do not need to check the entire "Time chain".

→ Validators are paid to order and check.

## Calculations sections

→ Wether / Stats.

→ Poisson / Reliability Model.

TBD later.

Need to model propagation

—SEIR.

—see virus & epidemic.

## Privacy

Not and will not be anon

Those criminal awards are the bone

of most systems.

— must kill off crime.

Privacy is not Anon.

We do need to isolate PTI.

Not like Visa

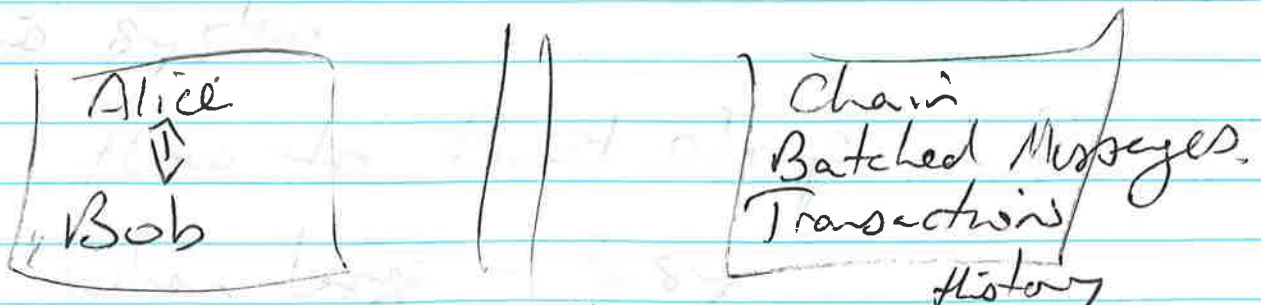
HIPAA  
etc.

look at Firewalling the system.

Users are able to exchange

identity But like the ASX

(NYSE etc) ticker - the public validate  
anything but without recourse to send  
the ID of the parties.



Known & Shared

Private & ID  
not available.

→ Not like PCP.

Keys are Not reused.

$P(A)_0$  = not shared (ID on PKI-CA)

$$P(A)_1 = P(A)_0 + P_{AB}$$

$P_{AB}$  known by A+B?

$P(A)_1 \leftrightarrow P(B)_1$  exchange

A+B can prove the other

But A+B not linked publicly

To  $P(A)_0$  or  $P(B)_0$ .

→ so ID is private

→ Need to sort the finances of this system.

How to Bootstrap it?

When large - Easy

Small → Ugh - Vulnerable

So much to do.

Alan → will BDO find systems?

Lessons → would be a means to stop what occurred.

World Centre bet of Sporting Bet are a token?

Need to see GCS + all other games co's also - wow.

also seek ideas in SCADA

- IOT - power etc.

LLM Topic -

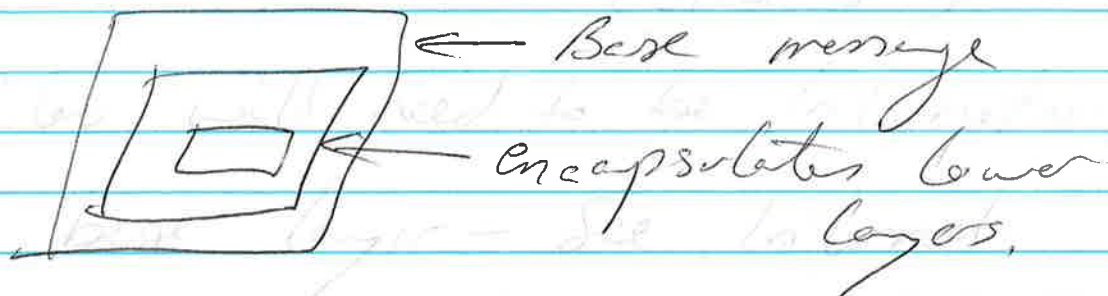
Internet Intermediaries.

We need to write how the Internets are - covered under law. How they can be constrained in have a legal framework for crimes online as money needs controls.

Need Protocol Versioning such that we can add layers.

- VER 0 (TCP)
- VER 1 (UDP)
- VER 2 (ICMP)
- VER 01 (HTTP)

- like IP  $\rightarrow$  layers in message.



Treeing + Recovery is far too big an area for my LL.M. PhD later?

The system needs a way to add Rules later - this needs to be distributed

$\rightarrow$  Money as a base - allow a token

for a separate Country

- UK, China, USA, Japan

$\rightarrow$  This will be encapsulated and able

to be exchanged in Bitcoin - See

P Wrayner - SWAPs - The atomic

swap ideas in his Game Book ✓  
likely need OT - Oblivious transfer  
would allow private transfer of  
assets on the system - Coin (A)  
Coin (B) ) swaps,

The Rules will need to be international  
at the base layer - see Internet  
intermediaries & liability.

- Common Carrier.

vs  
- Action.

The validators will need to act to  
freeze (WFO's) assets - easy as  
FIFO with ledger.

→ Alert the system.

We need an Alert Broadcast to  
stop the system moving a coin if it  
is validly frozen - fast - maybe a



Public vs Private - should have  
separate alert node system. A Court  
can sign a key - if valid court  
order - the coin can be tainted  
as invalid in jurisdiction X

Rules would cover restitution.

As the Validators can add  
code - code can be altered if the  
majority of validators agree - the  
commercial nodes are bound under  
law - with an audit record.

Tracing is simplified (Not like  
Blinded systems).

# Validators are a lot ~~like~~ like  
ISPs / PSPs - Payment validation  
as a distributed clearing house - Not  
and honest as all these guys are  
Public.

Public vs Private - child Porn / Terrorism  
CCM Dissertation Finding issues

Must cover IP + Internet law

The proposal is ok, the structure is ok - Need to get a draft by EOM Oct.

Alert is simple - send a message to all nodes - if a node or a user sees the alert - hold ~~to~~ and Freeze - who wants a tainted money!  
We can use the same broadcast to send such messages but later can expand this and add other non constant rules.

The rules are important.

What is needed is a means to act on a WORM.

Oracle — SANs, courses.

WORM. . Talk to Alon re  
write once read many.

Us clients are doing accounts not  
(Enron) on Oracle with the flags set  
to stop deleting records — they could  
use a WANC B tape.

— Once in  
Always in

Set change  $\Rightarrow$  a new record added  
to the tape — the chain is altered as  
a valid record sets why a change is  
made

So —  $A(\phi) \rightarrow C(i) \rightarrow A(i)$   
 $\rightarrow B(i)$ .

Here  $A$  has asset  $(\phi)$ .

$C$  issues an order and this  
is written to the chain.

The order allocates  $A(0)$  to  $A(1)$   
or  $B(1)$ .

So - the coin is now split by the terms of an order.

Too much far now - Not PoC.

But must get means to allow the validators to follow court rules or a court will simply rule the validator illegal.

The time chain is a law system.

The Rules are enforced by the validators - who act ~~are~~ as responsible Corporate citizens as they are Public

Important Users are, Private  
Validators are Not

Validators are utterly Not private  
as this scales — all they do  
— all they can  
— where they are.

All is seen — nothing a validator  
can do can be hidden — they have  
no clothes.

So — Validators will follow  
rules

OR they will be Fucked!

This Solves the issue of freezing  
restitution

Validators are under the  
Thump.

But Global law —

→ few crimes are global  
in nature.

→ International Enforcement.

The rules allow restitution (where economically justified)

The validators just after the code.

→ Version 2

Need Lynn's Paper & Work

"Corporate Social Responsibility"

The validators have no PII as the

receiver generates a new key pair and provides the public key to the sender just prior to signing.

Sender's PII & Pseudonym are no issue

[A & B] identities.

↓  
Template addresses.

OK Fashion law enforcement & tracing still will work and we save all the costs of managing private data.

For small transactions, the cost of an attack is low but the cost to the validator are high.

The only double-spend is where the validator acts to add the double spend - either they are a party or they are complicit. Instant with small risk.

- but a signed transaction  
- this means the receiver has an action and if not small - law  
Attacker is cheque fraud - but with a signed public audit & evidence trail.

→ A can be dlobbered in by B.

Law can then freeze assets.

A will have a signed transaction to two parties - this would be

Saved as an alternate chain history.

→ not forever - but long enough.  
As the keys are not reused an attacker  
cannot plan the attack in advance.

More if B sends the message  
Then B wins as the probability of A's  
message getting to C ~~is~~ and outpacing  
B's is based on an exponentially  
decreasing race.

More B could see A's message to  
C, know A is a cheat and stop  
the payment - keep the goods but  
maybe get paid - Coin does not pay  
with a time chain of blocks of  
batched transaction messages.  
The closer the batches - the more secure.



The receiver is alerted to the senders cheating in mere seconds - this could be better as the validators improve / professionalise.  
The only real attack - An attacker could try and change one of his own transactions to do cheque fraud and take back a payment of money he has just spent.

No Fed / Central Bank infinite printing ether as this is

1) ~~Global~~ Global.

2) Publicly Auditable.

This idea could allow DAATS  
CAATS

To be AI + automated - Audit will be about advice + classification again not the crap we are doing

Need to discuss with Neil & Alan.

IF BDO starts to act as a Validator  
this would get around early issues as  
an "issuer". They are tokens - commodity  
but with exchange value - not legal  
tender - But could open up a path to  
have banks use the chained block  
system in order to have perfectly  
honest auditable Fiat money.

- ~~Batched~~ Batched Coin

↓  
Fiat negotiable instrument.

→ tokenised USD - by Fed.

but - Central Banks are  
now publicly auditable - all the  
people see the games - no more  
secrets.

Extended - a log could be in messages.



each log in a merkle tree to collapse - but eg root logs are not collapsed - By value,

IF this works

I will get Both -

Partnership @ BDO

Professorship.

— Set!

Aura, et al 2000

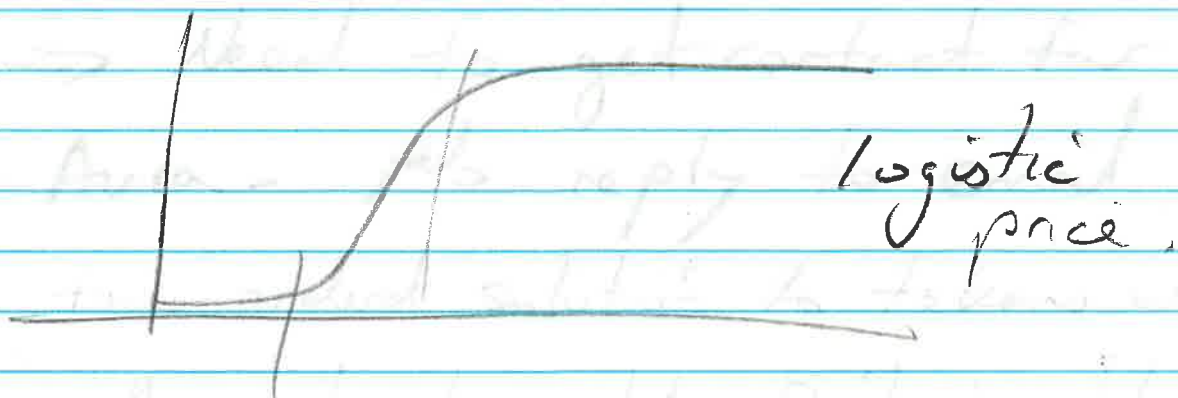
Dos Resistant Auth. with Client Proof.

T. Aura and others have a good idea of a client proof. They do not understand economics. They have all systems grinding which slows this to botnets & makes criminals have an advantage.

The idea is sound - the proof - really good - SHA 256 version (replace SHA1) and this is the evidence to show work in our chain.

The resources are best in a market, a user can best show by buying a proof of work done by another party who sells to a (global) market so the price is reflected as the use - not system by.

System - In having a fixed token supply - the value of the token will be traded and a value will reflect market demand.



The client commits resources in the form of money - not just as an effort at time, A user will be expected to have one PC, a botnet can be millions - so the hypotheses of Aura & even Dwork & Naor (98) is flawed.

But a user can purchase a token at a ~~set~~ exchange valued / market rate and now - any dishonest / criminal

host is incentivised to sell tokens to honest users. This kills off the negative externalities of the Free Free Internet model.

→ Need to get contact for Aura - also reply to email

The time ordered solution to tokens will allow these to be sold if it is able to be exchanged by supply is limited - cap.

→ Gold is a Good Model.

In a manner - Validators are analogous to Gold Miners.

→ The subsidy could degrade in the same way.

Set in blocks - but a planned removal over time. like Gold, lots - easy at

the starts ~~to~~ laying about on the ground, then over time, it becomes more and more difficult.

Aura's Auth Protocol. (S4)

Better if we have my idea as a market token - also - a ledger is a log - so attackers can not delete logs.

Difficulty Adjustment.

→ Set as Stag Hunt

~~that~~ Need more on

- Stackelberg Games.

- Red Queen.

- Oligarchy.

If share based - leads to Rent seeking  
Aristocratic - what work was done

Not what is being done.

Share based system results in lower work  
& security. Rent seeking  $\rightarrow$  crime.

Botnets  $\rightarrow$  ~~se~~ mining to get future share.

Must have miners - aka validators, earn  
each batch of transaction messages.

Information IS Value.

$\rightarrow$  Token could link to selling  
Access (see extended Aura idea).

This use of a partial match is simple to  
implement. Aura's idea of the initial  
zeros in a hash puzzle being matched is  
also simple to adjust as the difficulty is  
modified. So, far better as a work  
measure. We can use the market to  
adjust the <sup>i</sup>ardence of provided work



The use of a subsidy does help (I hope) bring parties into the game. The validators act like gold miners getting Gold off the ground at first then, as this is all found, they need a harder & harder effort to stay in the game.

This should force the low performers out. As the system grows - small players with low powered machines and slow networks will be made redundant (though they are still users).

Only high end corporate systems, data centres and companies who are willing to invest in this Red Queen Game will remain. The end - A few very large players - (Pareto) and some small ones

That discover a reiche means to mine profitably.

→ The system can also support specialists

A piece of a puzzle may be used.

This is achieved with a hash of A hash (solves some other security issues as an aside).

$$\text{Puzzle} = H_1(H_2(x))$$

Now -  $P_1 = H_1(H_2(x))$  needs to be solved in full.

But Party A can order transactions when the system is large.

The batched messages are hashed and handed to B.

$$B \text{ solves } P_2 = H_2(x)$$

→ As we have used a tree hash

A can have all the details but a small amount of info.

B can know they will be Paid By A.  $\rightarrow$  We can ~~be~~ setup systems where A + B specialise

A in Propagation + ordering (Validation).

B in Proof of Work.

$\rightarrow$  Over time, this can become (evolve) into a far more specialised system.

Not A + B  $\rightarrow$  B + many layers of corporation (as we see with the Internet + intermediaries)  $\rightarrow$  This can fragment to all the layers of Redback + Spiber as I could not ~~not~~ solve in 2002-4.

The issues with China + other slow nets can be solved - area specialist + low cost

labor vs high end systems etc.

Ultrafast Consensus in Small-World Networks

Olfati-Saber (2005).

- The transmission of a new block of batched messages is a phase change - Validators move from the last block to the next one and start a new ~~bt~~ batch.  
→ 1000x more efficient than a regular complex network.

"Random Rewiring" - Watts & Strogatz (1998).

- If we restrict the size to a small characteristic length - propagation is robust and efficient.

We end with a solution to Byzantine general problems. As long as the honest majority agree - then the system is robust in its

Simplicity.

Consensus is defined in this manner -  
and the idea has been touted as a way  
of solving - sensor network consensus,  
- load balancing  
- swarms & flocks  
- Sync. of coupled oscillators.

So, logging (SSH etc), SCADA Control and the  
overlays using this will be defined solutions  
and not mere ideas, but do not see that

I can ~~pt~~ patent the time chain idea -

BDO Capital Team.

Talked To Judith Ryan and Sebastian

Stevens in Corp. Either I am not explaining  
my idea well (at all) or the base timechain  
is a ~~me~~ not something that I could patent.

They also have concerns - banking and  
issue licence - and do not think that

you would be able to have a set of validators who are nodes that can come & go - partnership defined by a probabilistic lottery.

Alan Granger remains supportive (but seems to be politically isolated).

Rama Patel / Sidney Lim  $\rightarrow$  Also do not think that a signed ledger of batched blocks as a timestamp is able to be patented.

Blocks are discovered in a pool such as Aura() in a poisson distribution. Each validator finds at a rate  $\lambda_i$  so, if we take a system of independent poisson processes - each finds at rates  $\lambda_i$  for  $N_i(t)$ . Once the system - ~~with~~ <sup>a</sup> validation nodes finds a solution to the Aura()

proof - the winner sends to all other nodes - at the point where a batch block is solved and the proof of work puzzle is completed, the next is to broadcast to all other validators. So there is a small difference to a pure SIR model  $\rightarrow$  as propagation is instant but validators will lose if this is too big  $\rightarrow$  so they will expend to minimise the time

$\rightarrow \lambda_i$  = solve ~~batch~~ puzzle  
 $p_i$  = propagation time

$p_i \rightarrow \phi$  as the validator invests and should be small. Where  $p_i$  is large the  $\lambda_i$  is reduced. So, for an inefficient propagator ( $\lambda_{eff} = \lambda_i + p_i$ ) where

$\lambda_{id}$  is the batch block as it is discovered and propagated to the majority of other nodes - not all. But - the more the other nodes - and the faster - the more likely that node (i) will win the prize (fees for validation of the block or batch or messages).

So, if  $N_i(t)$  are (j) independent Poisson processes,  $N(t) = N_1(t) + N_2(t) + \dots + N_i(t) + \dots + N_j(t)$ .

$\forall i \geq 1 + j$  the total # of validators.

j likely to end between 1000 to 100-000 nodes.  
→ all depends on the propagation & network tech at the time.

Note - When (i) has sent/broadcast the probe to all other nodes (or rather a



significant ~~number~~ number of them) the process ~~seems~~ to be ~~inf~~ independent. As ~~successes~~ any other node knows of the solution, the choice is  $\rightarrow$  mine and validate the old or new block. If the validator has more than 50% of the network - they can treat this as if they own it - but then they are also bound under strict law that will bind more than as a part of the group consensus.

For each miner (i) the process is thus (when the rules ~~to~~ are followed) a 2 party Poisson Process.

$$N(t) = N_1(t) + N_2(t) \quad \text{where}$$

$$N_1(t) = N_i(t) \quad \text{original (discover block puzzle)}$$

$$N_2(t) = N_{j \neq i}(t) \quad \text{all other validators combined -}$$

$$N(t) = N_1(t) + N_2(t)$$

$$\text{thus } \lambda = \lambda_1 + \lambda_2$$

So if (1) has  $\frac{1}{3}$ <sup>rd</sup> of the CPU power and  $p_i \approx \phi$  (fast propagation)

then  $\lambda_2$  has  $\frac{2}{3}$  total CPU. So if

(1) discovers at a rate ~~2~~ and (2)

discovers a solution at  $\lambda_2 = 1$  ( $\lambda = \lambda_1 + \lambda_2 = 2 + 1 = 3$ )

So far each solution/it works on

an average over time.

Now - this means if  $p$  is large the

$\lambda$  we obtain is a combination of CPU

and propagation time  $\Rightarrow$  So we again

have validators seeking to minimise  $p_i$

as the propagation time increases - so

when we talk about a Visa size

system of 50,000 Transactors or

messages a second, we need now to

think on the time to propagate  $\rightarrow$  but  
Validators will have most or all of the  
messages - the hash of which (with very  
negligible collision - assume zero) rates is  
small SHA1 (160) SHA2 (256), SHA384) etc

So, even a large (10MB plus - or even  
the XP windows limit of 4.3gb) could  
be ignored with the patch read for  
only the hash  $\rightarrow$  4.3GB as 160 to 256 bits  
(8bit - bytes)  
- See - Splitting (thinning) of Poisson  
Processes  
- Merging independent processes.

- MSTAT Notes.

Note must add section on competing  
processes. The process is more of competing  
SEIR<sub>2</sub> (epidemic) models when blocks are  
discovered at around the same time.

## Lightning Download.

Have tested (see 2006 Ridges Notes) the  
XP downloader - Lightning Download  
See - [www.lightningdownload.com](http://www.lightningdownload.com) by Headlight Software

Order (5696-2)

licence name - CRAIG S WRIGHT

licence code -

WRIGHT-J388U-EAHR-P9355-  
UPX2A

Will not end in PoC code - but in my  
Alpha test would be a good thing to add.  
The software allows -

Splitting up to 10 network - but

I have changed this to 25 on  
a server PC with multi CPUs & <sup>lots</sup> RAM  
Dell.

Recovery - parts, files & thus messages  
can be resent & broadcast  
from a stop/start.

With more RAM, a better network (or even to

split pipes - see checkpoint (load balance & Firewall software) I think that a server farm could handle a large batch today. A 4.3GB (limit to windows) message can be split ~~ing~~ into 250 parts and on a 1GBe pipe or even (10 x 100MBe) this could be sent in 10 seconds - at data centre levels.

at 50k messages a second, the hash matching on a CPU will be more important than the network.

→ so, — Matching Batches by Hash (#)  
— Sending Messages.  
→ Validating  
→ Store / order.  
— Puzzle Solver.

→ Hash based databases will save the messages (see Alkani) and serve these but the chain of hashes can be created on

Large fast host as needed - so many specialisations will occur as the system professionalises.

I expect this to be analogous to the ISP industry - Pegasus/Comcast etc and how these became a few large (Professional) Systems.

If the system works as expected the validators end as a distributed Clearing House - a mutual where profit is earned probabilistically. In effect - the system has a number of corporations acting as the <sup>undefined-floating</sup> nebulous competition based distributed Intermediary. Need to tie this into Mutual, association & early Partnership law as this is really a form of early corporate

structure in the UK etc.

I do not see a scale limit in this - unbounded  
→ as the system grows it should be able to handle IOT + SCADA messages and even logs (over lay network - need to add VERSION to code + script)

Using CASE statements - not efficient - But PoC is just PoC. when I move from the Alpha towards a more corporate model, I can look at something more efficient than CASE (threading vs race conditions) - not sure how to have all the script constructs run and be tested in parallel ~~order~~ rather than sequential, but some of the SASI SANS guys know good coders. Planning to take GSE(.Net) exam next year. This covers

security - but need to learn to make my code scale more.

Can look at the system as a series of micro-services & architect this as web platforms are doing - as we scale - more likely to be able to gain from this approach. As ISP's started as home systems the distributed intermediary network will specialise. Seeing even ISP's now become more specialised (DNS, Email & Web speedshots and not ISP's doing it all).

- see STAR Web Application Security Notes

GREM - still like using the C&C model of Botnets for this IRC is a simple method to bootstrap & can use ~~to~~ some of the malware code we analysed in this for



good - I like the irony of creating a system that makes crime less profitable using code from criminals that is designed for cybercrime. Serves the dishonest bastards right that they are helping me destroy them and their scummy industry.

Honest nodes profit more!

Can link this to GCA + QCF4 stuff as the timechain is an evidence trail & could end used as ~~a~~ evidence in court.

Gerardo & Chowell + Carlos Castillo-Chavez  
(2013)

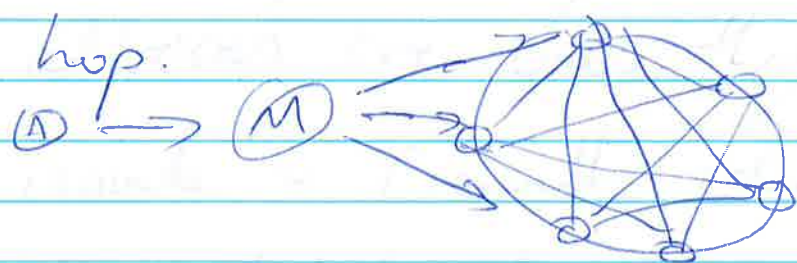
- Ch 2 - Worst-Case Scenarios &

- See 2.2 Fully Meshed transmission network. Epidemics,

The validators will seek to maximise connectivity

- So, merchants will want to know they are

Connecting to validator nodes - likely this will lead to the top "miner" getting more but this will be balanced as some merchants will send to lower miners and others to a random mix. Best with a random ~~and~~ range  $\rightarrow$  pick 8 say and check from others  $\rightarrow$  that is, send as the merchant to 8 validator nodes - and if 1000 miners there are 99% likely to send to all other miners in a single



So send to some at step 1

Send a validation at step 2.

- Now the miner knows if they cheat the other miners will report and the merchant

The sender A sends not to a PKI form address of the merchant  $\rightarrow$  ~~But~~ But a new key.

$P(M)_1 = P(M)_0 + P(MA)$  eg. so, the merchant could use a PKI identity and send a value (such as  $HMAC(X_A)$ ) to have

A & M generate a unique key and this is only a one time address w/ template.

A cannot send a "double-spend" with the merchant not knowing and as A signs the template, they know that the "change" addresses are ones they set. In this A & M

isolate & firewall identity completely from the validators/miners but the two contracting parties have evidence (admissible in court)

that is valid and can save the PII with less necessity to have all PII we do

Now in a visa world.

The "Worst Case" Scenario in Epidemics is the best case in our network and a giant network farms. Miners are naturally incentivised to connect to as many other nodes (validators) as they can as this helps them get a solution out as well. The need to solve a puzzle of batched messages and to be paid to not find a solution to the puzzle but to have the majority ~~in~~ in consensus that you have a solution before the ~~others~~ majority of others is the key. A miner who has a majority of other miners will likely also have miners on an alternate block that is just behind the 1st one defect as this

is the ultimate Game Strategy.

$t = 0 \Rightarrow M_1$  finds block puzzle  
(50% have it)

$t = 1 \Rightarrow M_2$  finds a block puzzle  
(25% of miners)

~~$t = 1$~~   $M_1$  (60% of miners)

$t = 2 \Rightarrow M_2$  gains some  
(30% of miners)

$M_1$  gains  
(70% of miners)

$t = 3 \Rightarrow M_2$  - loses some support  
(20% of miners)

$M_1$  - Gains  
(80% of miners)

$\rightarrow$  So as the mines see support for

$M_1 \rightarrow$  The SEIR model will allow

the mathematical ~~any~~ analysis in time of

what Blocks are still coming in a

"Competing Epidemics Model" - see

~~Influence~~ Influence Studies. (I(t)A vs I(t)B)

We can show, if  $M_1$  has 11% CPU power

&  $M_2$  has 30% CPU power that it

will be in  $M_2$ 's interests if  $M_1$  has managed to propagate blocks fast & now has  $> 50\%$  support. So even  $M_2$  with  $30\%$  CPU power fails if it does not ~~imp~~ immediately get a block ~~at this~~ puzzle discovery very fast - So no withholding strategy works - the validators are not going to end as the start and this forces professionalism & corporate roles to start to form.

Not all nodes in our graph are equal. More - it comes to the economics of the system - The cost of the node is a mix in time of capital costs - fast internet links & servers to hold all the data (and in time this could end as exabytes!)

and the immediate costs - staff, power etc and as power changes (day by day and hours in a day) nodes will globally shift in strength coming & going to maximise not revenue but total profit. This is an important aspect, the proof of work token now is an outsourced version of Arca's idea & one that has a floating value on some market.

- Need more time on "Bond Percolation processes" → studies of subsets of nodes

SIR is a simple idea but the propagation and validation time leads to SEIR models being more true.

As an overlay → the merchants will seek to maximise connectivity. At first the model

POC is best as a single node structure where one Alpha software does everything but in time we will need to move towards specialised systems.

likely that separate protocols for sending a message (merchant to the "miner" giant node structure), merchant validating the other (not sent to nodes) nodes have the transaction land as a separate check to having sent to the miner directly - this is a separate protocol as

$M \rightarrow V_1$  (send transaction)  
send the full message

$M \rightarrow V_2$  ( $V_1 \neq V_2$ ) is the hash  
of the transaction.

$V_2$  to  $M$  is a True/False.

True =  $V_2$  has the hash  
of the message.

False =  $V_2$  does not have it.



This forms a Bayesian belief network and the merchant can check (Reddy) fast if the message (with very low pre-purchase batch) probability will be in & accepted. We could have a miner attest  $\rightarrow$  and this now adds legal liability to a miner who is not honest. So -  $\sqrt{2}$  signs (maybe for a fee) an attestation  $\rightarrow$

$$S_1 = (\text{No TX}) \text{sig } v_2$$
$$S_2 = (\text{TX Good}) \text{sig } v_2$$

$\rightarrow$  Some Alert network for Validators

could be created in time to have a dishonest Validator ostracised and excluded and this will "punish" ill behaviour better than a "legal" process meaning only the worst cases will need to have laws & enforcement action - self regulating industry.

Need to find the ideal total ( $\lambda$ ) or  
batch period time - Note Poisson as an  
approx. So, with all the propagation  
→ to do this and minimise races and  
forks of this chain, we need a large  
enough time (even on batches of 100's of  
Gigabytes as this may end in a decade  
(if it works))

Must run scenarios.

→ Cannot be under 5 mins.

→ 20 to 30 mins is too slow.

→ Simple is best - so simple way to have  
the parties to know.

Values to test - 6 min // 10/hr  
- 10 min // 6/hr.  
- 12 min // 5/hr.

Must also look at how we can set the

puzzle to remain (→ period) - about the same.

→ long game period.

→ This is a Game, a zero sum game.

if  $V_1$  cheats, the same # of batch puzzle & rewards must be done in the set (far larger ~~that~~ than puzzle period).

well and - try 2 weeks  
2 weeks  
2 x Month  
1 x Month

→ if you have 10000 blocks a month every month, then if  $V_1$  cheats and loses a reward, there should still be 10000 valid batches that month.

→ Her two seedboxes - MA, ARIMA.

- Need to check models - to have a

difficulty that remains close to the same.

Also, we can expect the system to be able

to form a base layer protocol - like Internet with separate messages & templates doing all forms of non-cash transfers.

This can be a separate overlay that is linked by a set of hashes or other puzzles in code. Forth should do this well and allows us to try the WANG-B concept.

The time chain acts to stop all double spends, order (chronologically) messages and to (most importantly) pay the validators for this while being a micro payment system - in time, it could be that channels of thousands of a ~~sta~~ cent at a time are exchanged where trust is limited to 'credit' cents per exchange and thus the

SANS - CSE Malware as a target.

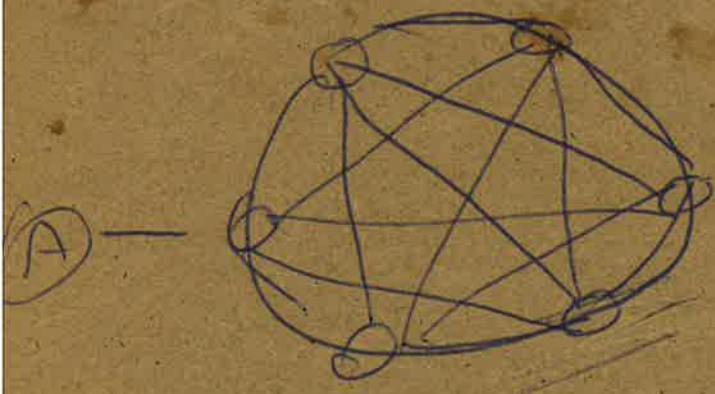
- Need to add this into my study schedule

- AIM for a year away - 2008 exam.

CSE-C Done - Can I do the (3) in 3 years - ?

- What will BDO allow for <sup>goal</sup> time/costs?

SEIR Rayner? others in MSTAT medical stream.



of offline also.

So A + B can find + B can check after time

Not as good as as IP to IP with valid but a gateway ~~to the~~ ~~firewall~~

~~Non Intermediary E-cash~~

~~E-cash with mutualised intermediaries~~

~~Cash claim~~

~~Time claim~~

~~Time coin~~

~~Byte coin~~

~~Byte cash~~

~~Digital Cash without trusted  
Third Parties~~

~~Electronic Cash without trusted  
Third Parties~~

Negotiable commodity  
Based exchange  
system