

# Blockchain and the Real Challenges of Building IT Systems

Martin Walker

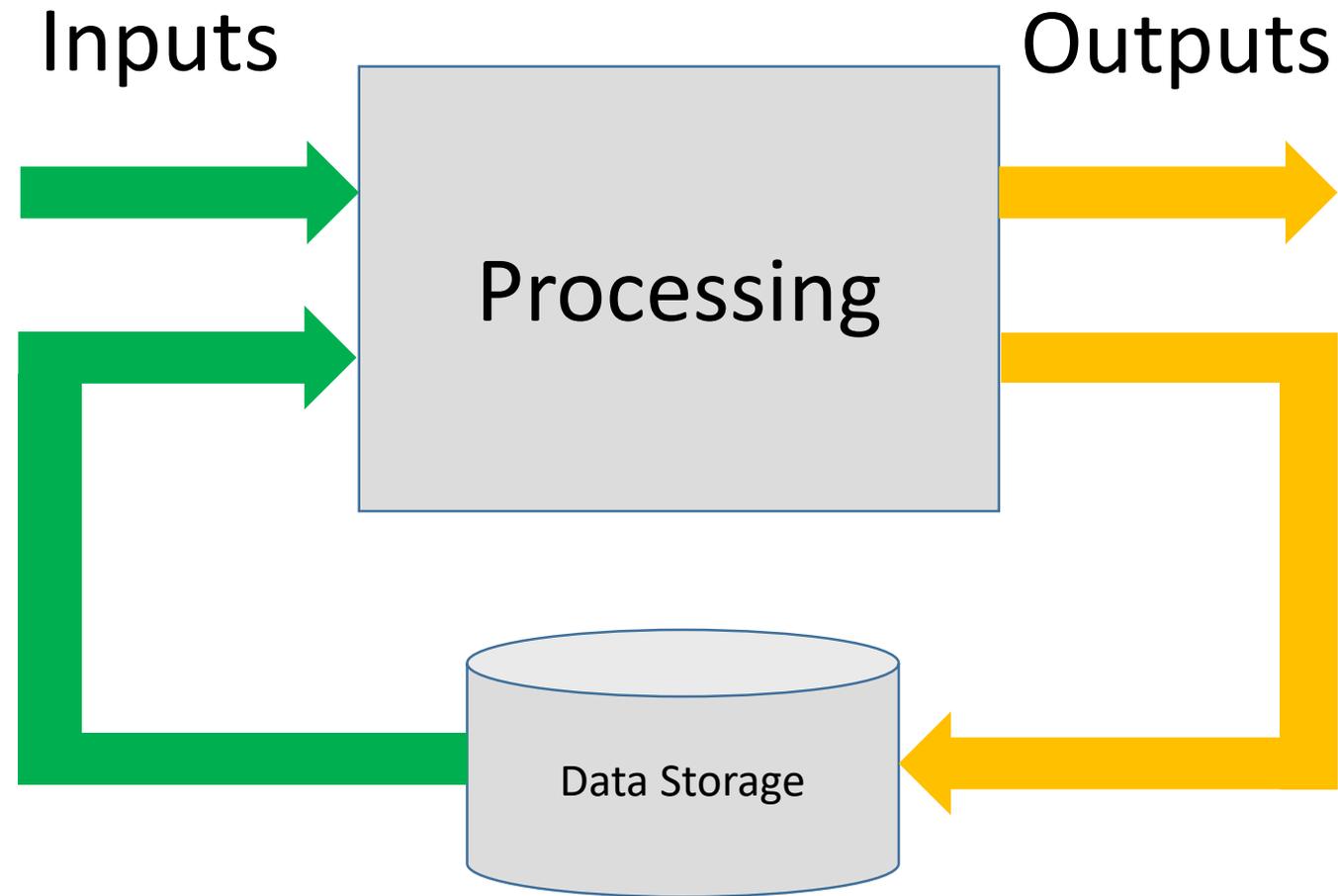
Amelia Island, Florida

May 20th 2019



ev·i·dence·based  
A focused approach to lead  
nact and to better tell its story  
-based ev·i·dence  
design and

# IT Systems – Made Simple



ev-i-dence-based  
A focused approach to leade  
nact and to better tell its story  
-based ev-i-dence  
design and

# Making Pancakes – Same Principles

## Inputs



## Processing

1. Put the flour, eggs, milk, 1 tbsp oil and a pinch of salt into a bowl or large jug, then whisk to a smooth batter. Set aside for 30 mins to rest if you have time, or start cooking straight away.
2. Set a medium frying pan or crêpe pan over a medium heat and carefully wipe it with some oiled kitchen paper. When hot, cook your pancakes for 1 min on each side until golden, keeping them warm in a low oven as you go.
3. Serve with lemon wedges and sugar, or your favourite filling. Once cold, you can layer the pancakes between baking parchment, then wrap in cling film and freeze for up to 2 months.

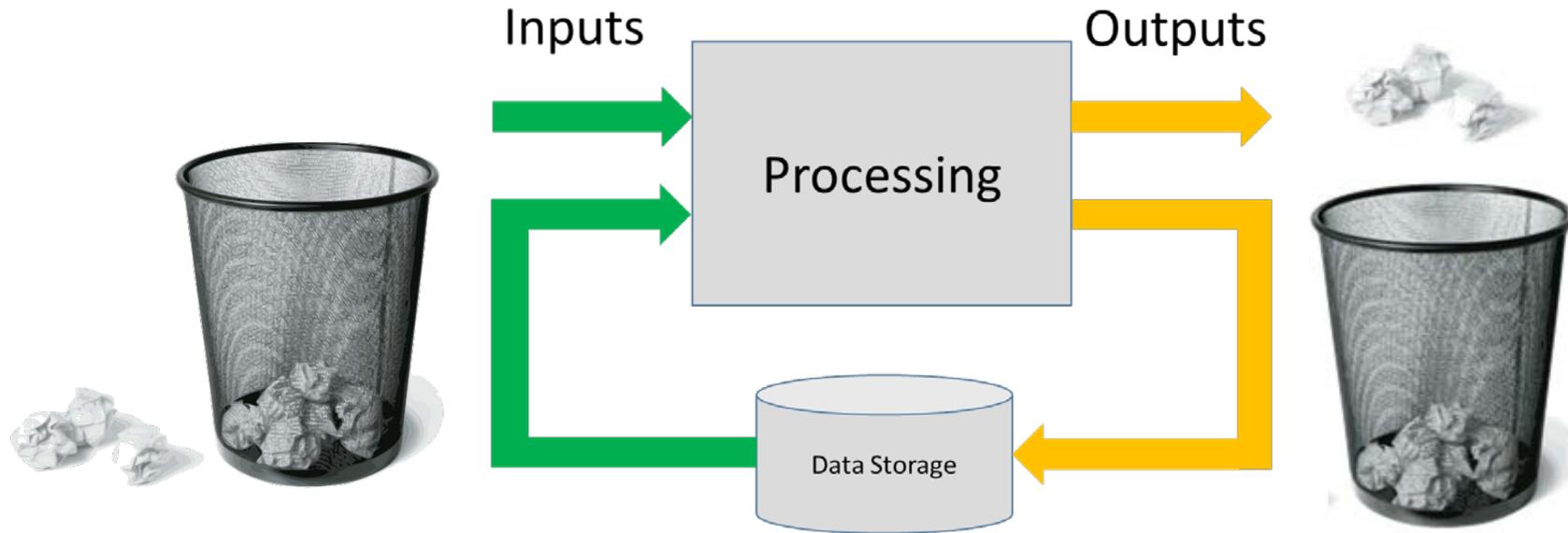


## Outputs



ev-i-dence-based  
A focused approach to lea  
nact and to better tell its story  
-based ev-i-dence  
design an

# Garbage In – Garbage Out

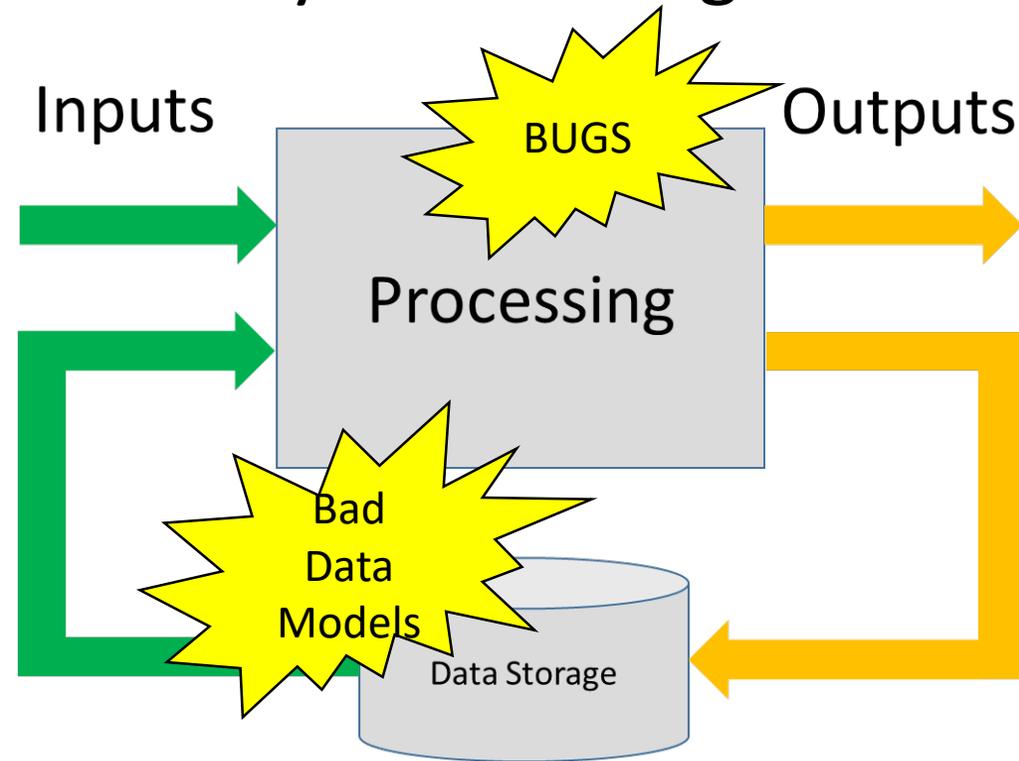


Put garbage into a system and you are likely to get garbage out. Worse case the garbage (or bad inputs) in combination with lack of programming logic can cause the whole system to crash.

Where does the “garbage” come from?

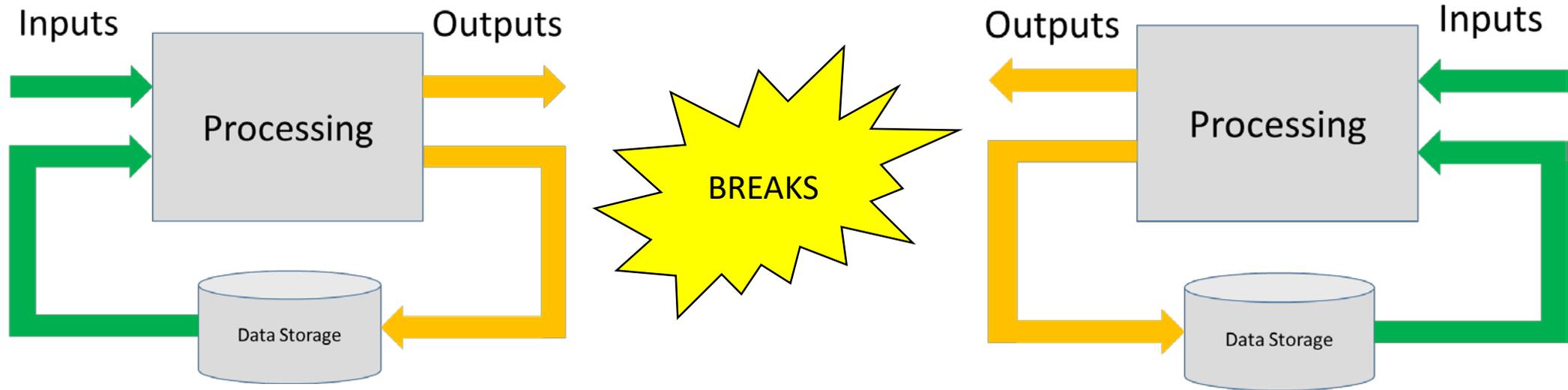
- Human error
- Another system feeding in incorrect data
- Previously generated data stored incorrectly within the system
- Criminal activity

# IT Systems – Bugs



- Having the wrong logic implemented in a program, more commonly known as a “bug” can be due to both implementing programming logic incorrectly, functional gaps or failing to deal appropriately with bad or missing data
- Data that is stored in a system needs a structure so the system or anyone querying the system can understand what it represents. This is not always done correctly. People often force data into systems that does not fit

# Consistency Between Systems



Different parties to a transaction (or even different systems belonging to the same party) can easily end up with different views of the truth. This results from some basic problems

- Inputs for one or both parties can be wrong
- One party may have a more up-to-date view of the truth
- The way data is stored about the truth may be different leading to different results
- The processing logic may be different

# Accurate Representation of the Real World



<b>ID</b>	233301223
<b>DataTime</b>	05/05/2019 12:03
<b>InputUser</b>	Martin
<b>Type</b>	Floribunda
<b>Color</b>	Yellow
<b>Origin</b>	UK
<b>Supplier</b>	English Roses Ltd

- Input errors, programming errors or fraud can mean that the real world object is not the same as the data representation
- With complex supply chains there are multiple opportunities/incentives such as switching or forging labels or paperwork



**FIRST BANK OF WIKI**  
 1425 JAMES ST. PO BOX 4000  
 VICTORIA BC V8X 3X4 1-800-555-5555

CHEQUING ACCOUNT STATEMENT  
 Page : 1 of 1

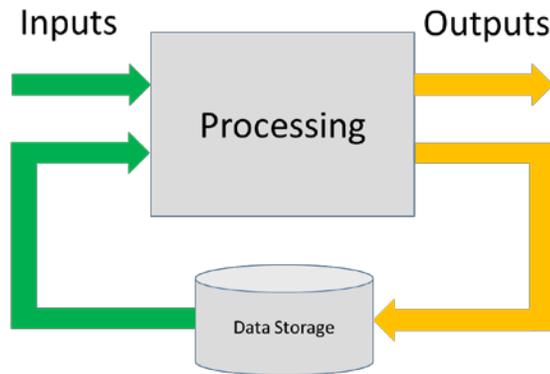
JOHN JONES  
 1643 DUNDAS ST W APT 27  
 TORONTO ON M8K 1V2

Date	Description	Ref.	Withdrawals	Deposits	Balance
2003-10-08	Previous balance				0.55
2003-10-14	Payroll Deposit - HOTEL			694.81	695.36
2003-10-14	Web Bill Payment - MASTERCARD	9685	200.00		495.36
2003-10-16	ATM Withdrawal - INTERAC	3990	21.25		474.11
2003-10-16	Fees - Interac		1.50		472.61
2003-10-20	Interac Purchase - ELECTRONICS	1975	2.99		469.62
2003-10-21	Web Bill Payment - AMEX	3314	300.00		169.62
2003-10-22	ATM Withdrawal - FIRST BANK	0064	100.00		69.62
2003-10-23	Interac Purchase - SUPERMARKET	1559	29.08		40.54
2003-10-24	Interac Refund - ELECTRONICS	1975		2.99	43.53
2003-10-27	Telephone Bill Payment - VISA	2475	6.77		36.76
2003-10-28	Payroll Deposit - HOTEL			694.81	731.57
2003-10-30	Web Funds Transfer - From SAVINGS	2620		50.00	781.57
2003-11-03	Pre-Auth. Payment - INSURANCE		33.55		748.02
2003-11-03	Cheque No. - 409		100.00		648.02
2003-11-06	Mortgage Payment		710.49		-62.47
2003-11-07	Fees - Overdraft		5.00		-67.47
2003-11-08	Fees - Monthly		5.00		-72.47
*** Totals ***			1,515.63	1,442.61	

- The record of the existence of almost all financial assets (including funds in a checking account) is digital
- But those records ultimately represent the real world, legally enforceable relationship between “Obligor” and “Obligee”
- This is not the same as infinitely duplicable digital assets such as MP3s

ev-i-dence-based  
 A focused approach to lea  
 nact and to better tell its story  
 -based ev-i-dence  
 design and

# Security



## Ability To Use System

## Ability to change code

## Access to Data

- Need to control who can use systems, who can change the code or data models and who has access to data
- Security is not just about keeping out bad actors it is about protecting people from making accidents

ev-i-dence-based  
A focused approach to lea  
nact and to better tell its story  
-based ev-i-dence  
design an

# ..and Blockchain Adds?

Problem	Real World/Logical Solution	What Blockchain adds?
Processing Logic i.e. Bugs	Train people to program, do analysis to try make sure system is doing and test, test, test.	Smart Contracts are programs, written in programming languages and frequently contain bugs. If a program is running decentralised and goes wrong no one can stop it.
Data Models	Train people to design things, we test the systems that encapsulate data models and we work to agree common standards across systems and the relevant firms	Still need to agree data models and get consistency. The enthusiasm for blockchain can be a catalyst to get people to talk about standards.
GIGO	Have controls around what goes into system, who can use the system (and make sure they are appropriately trained) build in validation of inputs	You have to use same systems and techniques to control what goes in. Blockchain alone does nothing to remove the problem the GIGO problem.
Consistency Between Systems	Agree transactions on a common system and feed other systems from golden record. Alternative attempt to use the same system and/or data models	Everybody essentially uses clones of the same system but you still get timing issues, you still need to feed into other systems. This type of model can work but it is inherently computationally inefficient. It can also be implement using traditional technologies
Accurate Representation of the Real World	Control how data is captured, audit the supply chain, use reputable suppliers.	Same techniques but do it on the blockchain
Security	Only allow appropriate people to have access to system. Keep out everyone else. Periodically validate permissions and test the security checks. Keep vendor provided systems up to date.	Make it evident if someone has tampered with data. Sometimes distribute data to wide group but encrypt it. Inherent problems come if all data is distributed to all parties. The irreversibility of transactions on a de-centralised blockchain is one of the fundamental causes of cryptocurrency thefts.

evidence-based  
 A focused approach to leading  
 impact and to better tell its story  
 evidence-based  
 design and

# Conclusion

- Blockchain type technologies do not fundamentally change or remove the key challenges faced in building an IT system
- Blockchain based/influenced systems can be used to implement new and innovative ideas but so can existing technologies
- Anyone faced with building, buying or integrating a new system cannot simply assume they should use a blockchain based system because it is new, better or in some way magical
- People still have to think, to define the problems they face and critically evaluate the evidence about the effectiveness of their technology options